Dell™

# Dell Management Plug-in for VMware vCenter Version 1.0.1 Update 1

## User's Guide

# Notes and Cautions

**NOTE:** A NOTE indicates important information that helps you make better use of your computer.

**CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.**

---

**Information in this document is subject to change without notice.**
**© 2011 Dell Inc. All rights reserved.**

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL™ logo, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, KACE™, FlexAddress™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core™ and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD®, the AMD logo®, and combinations thereof, are registered trademarks and AMD Opteron™, AMD Phenom™, and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat Enterprise Linux® and Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® is a registered trademark and SUSE ™ is a trademark of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter®, and vSphere® are registered trademarks or trademarks of VMWare, Inc. in the United States or other countries.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

**October 2011**

# Contents


1 Overview . . . . . 9

**Dell Management Plug-in for VMware vCenter** . . . . . **9**

**Key Features** . . . . . **9**

**How Does the Plug-in Help With vCenter Administration?** **10**

**Plug-In Features** . . . . . **10**

2 Plug-In Configuration . . . . . 13

**Security Roles and Permissions** . . . . . **13**

Data Integrity . . . . . 13

Access Control Authentication, Authorization, and Roles . . . . . 14

Privileges . . . . . 18

**Complete Configuration Wizard - Create System Connection Profiles** . . . . . **20**

Create and Assign Connection Profiles . . . . . 21

Events and Alarms . . . . . 25

Proxy Settings . . . . . 26

Schedule an Inventory Job . . . . . 26

Warranty Data Retrieval . . . . . 27

Deployment Credentials . . . . . 27

Firmware Repository . . . . . 28

OpenManage Server Administrator URL . . . . . 29

Immediately Run an Inventory . . . . . 30

Set Up an OMSA Trap Destination . . . . . 31

Download Firmware Updates and Make Available. 31
Configure Dell iDRAC Auto Discovery and Initial Start-up, and Disable/Enable User ID and Password 36

**NFS Share Configuration** . . . . . **39**

**Uninstalling Dell Management Plug-In for VMware vCenter 39**

**Upgrading Dell Management Plug-In for VMware vCenter 40**

Upgrading from Version 1.0 to 1.0.1 . . . . . 40
Upgrading from Trial Version 1.0.1 to Full Product Version 1.0.1 . . . . . 41
Upgrading Dell Management Plug-in from 1.0.1 to 1.0.1 Update 1 . . . . . 41
Upgrading Dell Management Plug-in using VCenter 5 42

3 End-to-End Hardware Management . . . 45

**Monitoring** . . . . . **45**
Configure Event and Alarm Settings . . . . . 45
Set up an OMSA trap destination. . . . . 46
View Events . . . . . 47

**Inventory** . . . . . **47**
Managing Connection Profiles . . . . . 48
Schedule and Run Inventory . . . . . 50
Display Server Hardware Configuration and Status 51
Display System Event Logs . . . . . 54

**Advanced Host Management** . . . . . **55**
Server Identification . . . . . 55
Server-Based Management Tools . . . . . 56
Proactive Systems Management . . . . . 56

**Warranty Retrieval** . . . . . **57**
Display Server Warranty Information. . . . . 57

Proxy Settings . . . . . 58

4 Zero-Touch Hardware Provisioning and Deployment . . . . . 61

**Hardware Prerequisites** . . . . . **61**

**Overview** . . . . . **62**

**Understanding Deployment Job Times** . . . . . **63**

**Server States Within the Deployment Sequence** . . . . **63**

**Configure a Hardware Profile** . . . . . **64**

Setting Collect System Inventory on Restart (CSIOR) on a Clone Server . . . . . 65

Create New Hardware Profile . . . . . 65

Managing Hardware Profiles . . . . . 68

**Configure a Hypervisor Profile** . . . . . **69**

Create New Hypervisor Profile . . . . . 70

Managing Hypervisor Profiles . . . . . 71

**Building a Deployment Template** . . . . . **72**

Managing Deployment Templates . . . . . 72

**Running the Deployment Wizard** . . . . . **73**

Managing Deployment Jobs Using the Deployment Job Queue . . . . . 75

**Server Security Settings for Deployment** . . . . . **76**

5 Firmware Updates . . . . . 79

**Enter Global Firmware Repository Location** . . . . . **79**

**Update Individual Server Firmware** . . . . . **80**

6 Management Plug-In Administration . . 83

**Web-based Administration Portal** . . . . . **83**

vCenter Registration . . . . . 83

Virtual Appliance Management. . . . . 85

Global vCenter Alert Settings . . . . . 88

Plug-in Database Backup and Restore . . . . . 89

**Console View** . . . . . **91**

Configure Network Settings . . . . . 91

Change Virtual Appliance Administration Password 91

Set Local Time Zone . . . . . 91

Reboot Virtual Appliance . . . . . 91

Reset Virtual Appliance to Factory Settings . . . . 92

Refresh Console Tab View . . . . . 92

ReadOnly User Role . . . . . 92

7 Troubleshooting . . . . . 93

**Upgrade** . . . . . **93**

**Common Questions** . . . . . **93**

**Bare-Metal Deployment** . . . . . **98**

Auto-Discovery and Handshake Prerequisites. . . 98

Hardware Configuration Failure . . . . . 98

Enabling Auto-Discovery on a Newly-Purchased System. . . . . 99

**Contacting Dell** . . . . . **100**

**Where to get additional help for this software** . . . . **100**

**Dell Management Plug-in for VMware vCenter Related information** . . . . . **100**

A Virtualization-Related Events . . . . . 103

Index . . . . . 111

# 1

# Overview

## Dell Management Plug-in for VMware vCenter

VMware vCenter is the primary console used by IT administrators to manage and monitor VMware vSphere ESX/ESXi hosts. In a standard virtualized environment, VMware alerts and monitoring are used to prompt an administrator to launch a separate console to resolve hardware issues. Today, using the Dell management Plug-In for VMware vCenter, administrators have new capabilities to manage and monitor Dell hardware within the virtualized environment, such as:

- Alerting and environment monitoring
- Single server monitoring and reporting
- Firmware updates
- Enhanced deployment options

## Key Features

Dell customers can use the Management Plug-In to perform:

- **Inventory**—Inventory key assets, perform configuration tasks, and provide cluster and datacenter views of Dell platforms.
- **Monitoring and Alerting**—Detect key hardware faults, perform virtualization-aware actions (for example, migrate workloads or place host in maintenance mode), and provide proactive resolution based on hardware events.
- **Firmware Updates**—Update Dell hardware to the most updated version of BIOS and firmware.

- **Deployment and Provisioning**—Create hardware profiles, hypervisor profiles, and deploy any combination of the two on bare-metal Dell PowerEdge 11th generation servers, remotely and without PXE—using vCenter.
- **Service Information**—Retrieve warranty information from Dell online.

## How Does the Plug-in Help With vCenter Administration?

Dell Management Plug-in for VMware vCenter provides additional virtualization functionality that supplements the current vCenter administration functions:

- Compresses tasks and adds management processes, such as firmware updates and bare-metal deployment, to the vCenter Server Administration Portal.
- Organizes deployment of multiple bare-metal servers without requiring Preboot Execution Environment (PXE).
- Provides additional intelligence (inventory, events, alarms) to diagnose server problems.
- Integrates with standard vCenter authentication, rules, and permissions.

## Plug-In Features

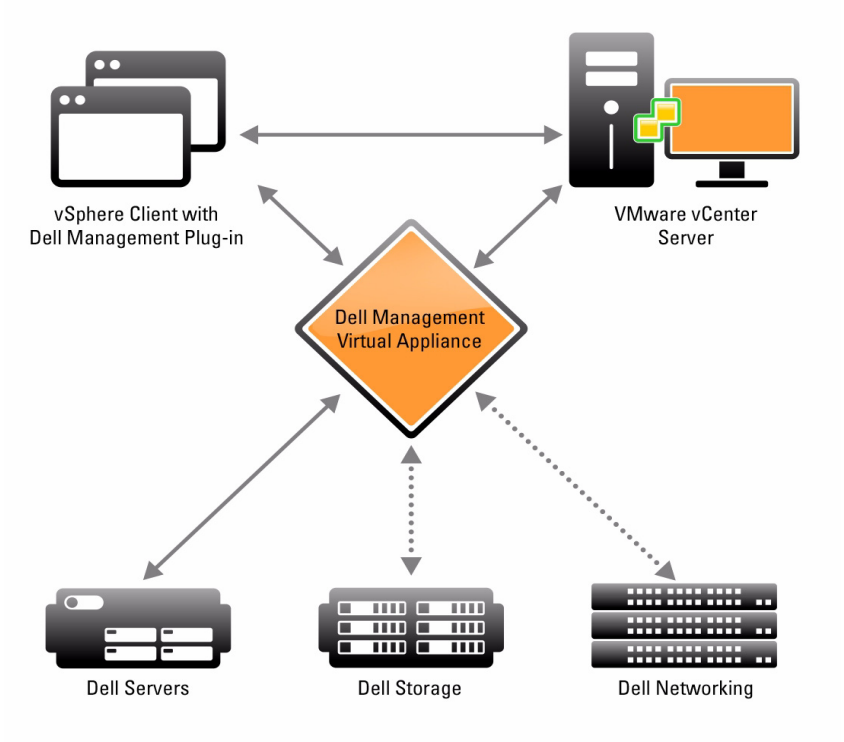
The following are high-level features of the Dell Plug-in for VMWare vCenter:

- Monitor Dell platforms using the standard vCenter event and alarm subsystem
- Perform advanced hardware management and configuration
- Perform zero touch deployment of hypervisors on bare-metal systems without using PXE
- Build hardware and hypervisor profiles
- Perform firmware updates
- Troubleshoot infrastructure issues
- Report at the Datacenter and Cluster view—export to CSV file

- Integrate plug-in capabilities with standard vCenter roles and permissions

The following diagram provide an architectural overview of a typical Dell Management Plug-In deployment, including the communication paths between the various components.

**Figure 1-1. Architecture Overview**



# 2

# Plug-In Configuration

The following sections provide step-by-step instructions for the plug-in initial configuration. Upgrade, uninstallation, and security role information is also covered in this chapter.

## Security Roles and Permissions

The Dell Management Plug-In encrypts and stores sensitive user credential information. It does not provide any passwords to client applications to avoid any improper requests that could lead to issues. The database back-ups are fully encrypted using custom security phrases, and therefore the data cannot be misused.

### Data Integrity

Communication between the Plug-in, virtual appliance, administration console, and vCenter is accomplished using SSL/HTTPS. The Plug-in can generate an SSL certificate used for trusted communication between vCenter and the appliance. It also verifies and trusts the vCenter server's certificate before communication and Plug-In registration. The Dell Administration Portal uses security procedures to avoid improper requests while the keys are transferred back and forth from the administration console and back-end services. This type of security causes cross-site request forgeries to not be successful.

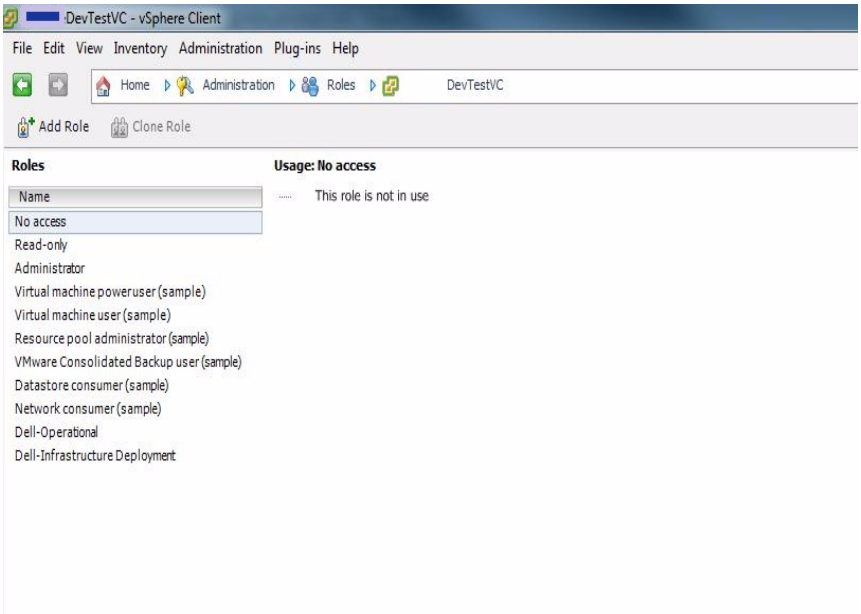
A secure administration console session has a five minute idle minute, and the session is only valid in the current browser window and/or tab. If the user tries to open the session in a new window or tab, a security error is created that asks for a valid session. This action also prevents the user from clicking any malicious URL that could try to attack the administration console session.

**Figure 2-1. Error Message**

## Access Control Authentication, Authorization, and Roles

The Dell Management Plug-In uses the vSphere client's current user session and the stored administration credentials for the appliance to perform vCenter operations. The administration and the appliance consoles are also accessible by using a strong administration password. The Plug-in uses the vCenter server's built-in roles and privileges model to authorize user actions with the appliance and the vCenter managed objects (hosts and clusters). The Plug-in creates the roles and privileges displayed in Figure 2-2 during registration.

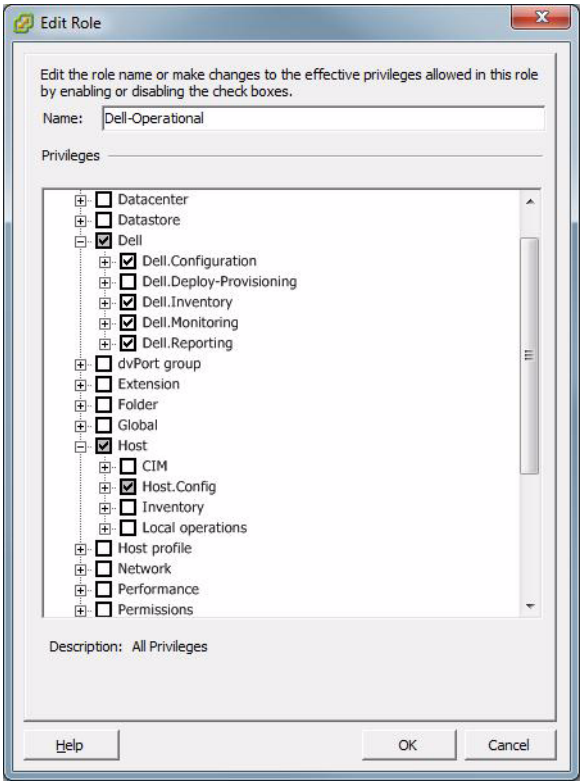
**Figure 2-2. vCenter Roles and Privileges**




### Dell Operational Role

Contains the privileges/groups required to do general appliance and vCenter operations including firmware update, hardware inventory, restart host, put host to maintenance mode, create vCenter task.

**Figure 2-3. Dell Operational Role**




This role contains the following privilege groups and individual privileges.

- Privilege Group - Dell.Configuration
  - Privilege - Perform Host-Related Tasks, Perform VCenter-Related Tasks, Configure SelLog, Configure ConnectionProfile, Configure ClearLed, Firmware Update
- Privilege Group - Dell.Inventory
  - Privilege - Configure Inventory, Configure Warranty Retrieval, Configure ReadOnly
- Privilege Group - Dell.Monitoring

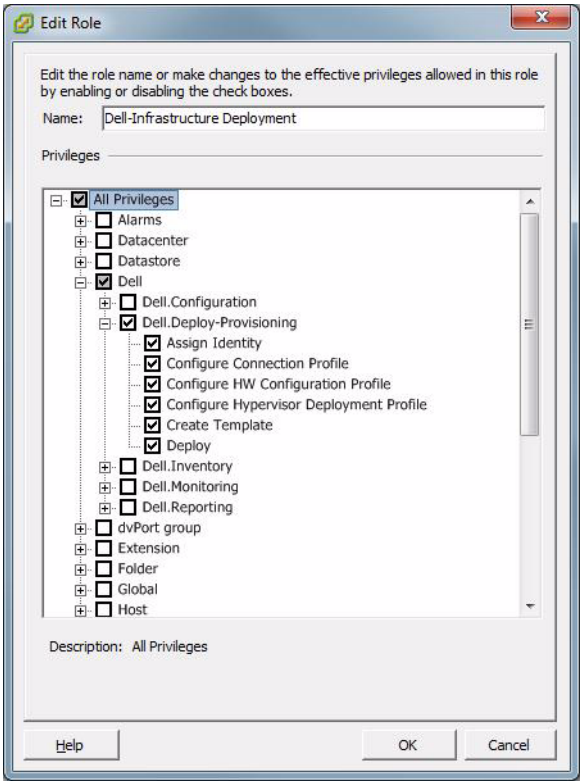
- Privilege - Configure Monitoring, Monitor

- Privilege Group - Dell.Reporting (Not used)
  - Privilege - Create a Report, Run a Report

### Dell Infrastructure Deployment

This role contains the privileges specifically related to the hypervisor deployment features.

**Figure 2-4. Dell Infrastructure Deployment Role**




This role contains the following privilege groups and individual privileges.

- Dell.Deploy-Provisioning

- Privilege - Create Template, Configure HW Configuration Profile, Configure Hypervisor Deployment Profile, Configure Connection Profile, Assign Identity, Deploy

## Privileges

Every action performed by the Plug-in is associated to a privilege. The following sections list the available actions and the associated privileges.

- Dell.Configuration.Perform VCenter-Related Tasks
  - Exit and enter maintenance mode
  - Get the vCenter user group to query the permissions
  - Register and configure alerts, for example enable/disable alerts on the event settings page
  - Post events/alerts to vCenter
  - Configure event settings on the event settings page
  - Restore default alerts on the event settings page
  - Check DRS status on clusters while configuring alerts/events settings
  - Reboot host after performing update or any other configuration action
  - Monitor vCenter tasks status/progress
  - Create vCenter tasks, for example firmware update task, host configuration task, and inventory task
  - Update vCenter task status/progress
  - Get host profiles
  - Add host to data center
  - Add host to cluster
  - Apply profile to host
  - Get CIM credentials
  - Configure hosts for compliance
  - Get the compliance tasks status
- Dell.Inventory.Configure ReadOnly
  - Get all vCenter hosts to construct the vCenter tree while configuring connection profiles

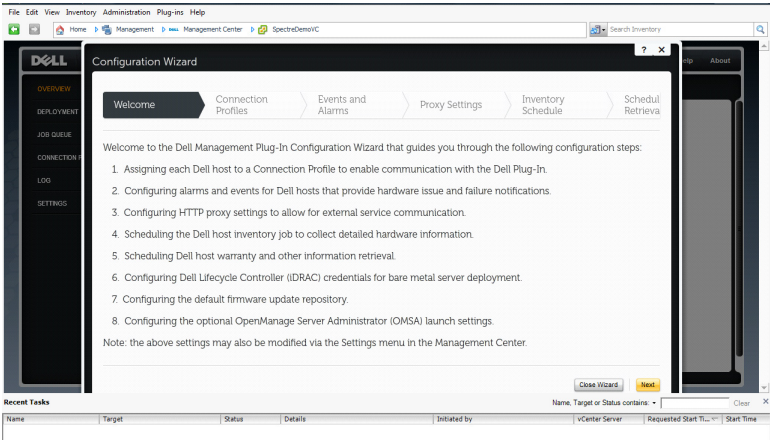
  - Check if the host is a Dell server when the tab is selected
  - Get the vCenter's Address/IP
  - Get host IP/Address
  - Get the current vCenter session user based on the vSphere client session ID
  - Get the vCenter inventory tree to display the vCenter inventory in a tree structure.
- Dell.Monitoring.Monitor
  - Get host name for posting the event
  - Perform the event log operations, for example get the event count, or change the event log settings
  - Register, unregister, and configure events/alerts
  - Receive SNMP traps and post events
- Dell.Configuration.Firmware Update
  - Perform firmware update
  - Load firmware repository and DUP file information on the firmware update wizard page
  - Query firmware inventory
  - Configure firmware repository settings
  - Configure staging folder and perform update using the staging feature
  - Test the network and repository connections
- Dell.Deploy-Provisioning.Create Template
  - Create, display, delete, and edit deployment templates
- Dell.Configuration.Perform Host-Related Tasks
  - Blink LED, Clear LED, Configure OMSA URL from the Dell Tab
  - Launch OMSA Console
  - Launch iDRAC Console
  - Display and clear SEL log
- Dell.Inventory.Configure Inventory
  - Display system inventory in the Dell Tab

- Get storage details
- Get power monitoring details
- Create, display, edit, delete, and test connection profiles on the connection profiles page
- Schedule, update, and delete inventory schedule
- Run inventory on hosts

## Complete Configuration Wizard - Create System Connection Profiles

1. Click the **Dell Management Center icon**.
2. The configuration wizard displays. The following settings are required:
   a. Create and assign a connection profile to a single host for Plug-in communication; a connection profile may be assigned to more than one host.
   b. Configure default events and alarm settings.
   c. Configure any required HTTP proxy settings used to access Dell online.
   d. Schedule an inventory job to gather managed Dell Host server information.
   e. Schedule a job to retrieve warranty and other information.
   f. Enter the URL for the OpenManage Server Administrator (OMSA) Web user interface so that it can be launched from within vCenter.

**Figure 2-5. Management Center Configuration Wizard**


File Edit View Inventory Administration Plug-ins Help
Home Management Management Center SpectreDemoVC
Search Inventory
DELL
Configuration Wizard
OVERVIEW
DEPLOYMENT
JOB QUEUE
CONNECTION
LOG
SETTINGS
Welcome
Connection Profiles
Events and Alarms
Proxy Settings
Inventory Schedule
Schedul Retrieva
Welcome to the Dell Management Plug-In Configuration Wizard that guides you through the following configuration steps:
1. Assigning each Dell host to a Connection Profile to enable communication with the Dell Plug-In.
2. Configuring alarms and events for Dell hosts that provide hardware issue and failure notifications.
3. Configuring HTTP proxy settings to allow for external service communication.
4. Scheduling the Dell host inventory job to collect detailed hardware information.
5. Scheduling Dell host warranty and other information retrieval.
6. Configuring Dell Lifecycle Controller (IDRAC) credentials for bare metal server deployment.
7. Configuring the default firmware update repository.
8. Configuring the optional OpenManage Server Administrator (OMSA) launch settings.
Note: the above settings may also be modified via the Settings menu in the Management Center.
Close Wizard
Next
Recent Tasks
Name, Target or Status contains:
Clear
Name
Target
Status
Details
Initiated by
vCenter Server
Requested Start Ti...
Start Time

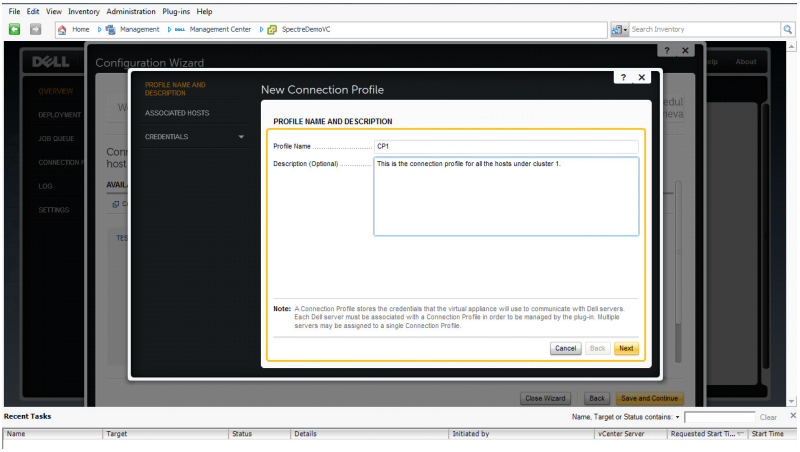
3 Complete the configuration wizard by entering the required information; see the following sections for more details.

## Create and Assign Connection Profiles

1 Click **Create New** in the configuration wizard. The new connection profile wizard displays.

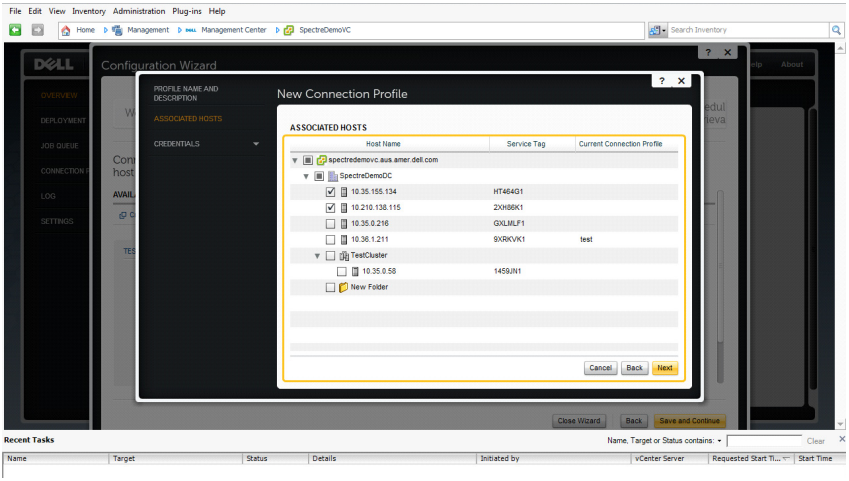
2 Enter a name and description (optional) for the new connection profile, then click **Next**.

**Figure 2-6. New Connection Profile Wizard**




3 Select hosts that have the same iDRAC and ESX/ESXi host credentials.

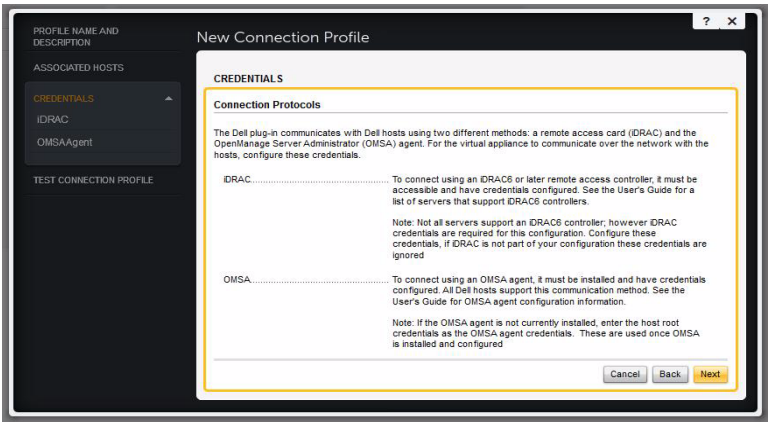
**Figure 2-7. Select Hosts**




4 A **Credentials** window is displayed. Information on the required iDRAC and OMSA credentials is provided. Click **Next**.

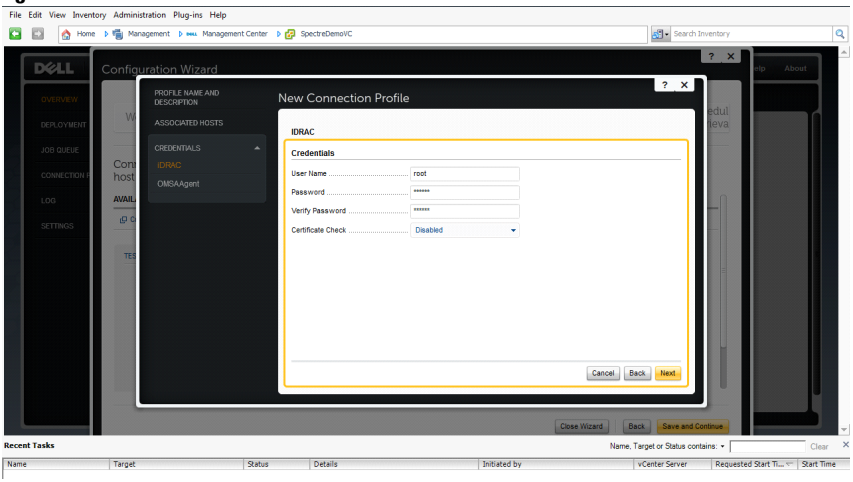
**NOTE:** The OMSA credentials are the same credentials used for ESX and ESXi hosts.

**Figure 2-8. Credential Window**


PROFILE NAME AND DESCRIPTION
ASSOCIATED HOSTS
CREDENTIALS
iDRAC
OMSAAgent
TEST CONNECTION PROFILE
New Connection Profile
CREDENTIALS
Connection Protocols
The Dell plug-in communicates with Dell hosts using two different methods: a remote access card (iDRAC) and the OpenManage Server Administrator (OMSA) agent. For the virtual appliance to communicate over the network with the hosts, configure these credentials.
iDRAC
To connect using an iDRAC6 or later remote access controller, it must be accessible and have credentials configured. See the User's Guide for a list of servers that support iDRAC6 controllers.
Note: Not all servers support an iDRAC6 controller; however iDRAC credentials are required for this configuration. Configure these credentials, if iDRAC is not part of your configuration these credentials are ignored
OMSA
To connect using an OMSA agent, it must be installed and have credentials configured. All Dell hosts support this communication method. See the User's Guide for OMSA agent configuration information.
Note: If the OMSA agent is not currently installed, enter the host root credentials as the OMSA agent credentials. These are used once OMSA is installed and configured
Cancel
Back
Next

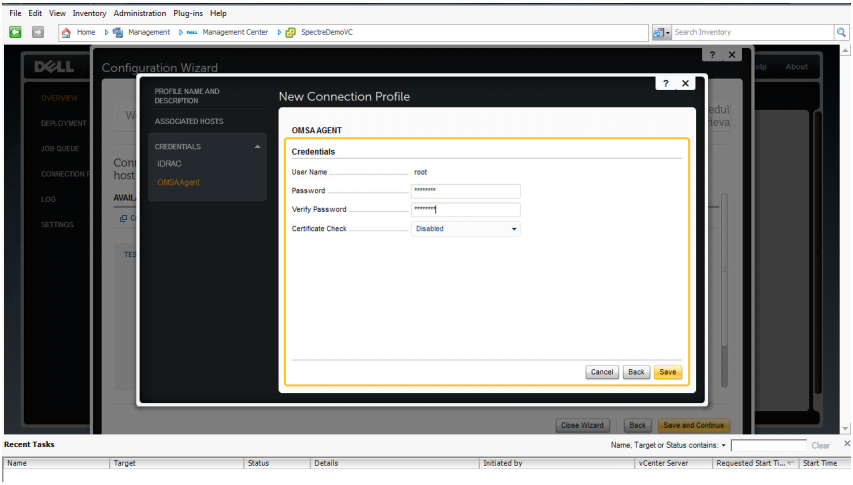
5 The **iDRAC Credential** window is displayed. Enter the iDRAC administrator user name and password, and click **Next**.

**Figure 2-9. Enter iDRAC Credentials**




6 The **OMSA Agent Credential** window is displayed. Enter the OMSA agent root password and click **Next**.

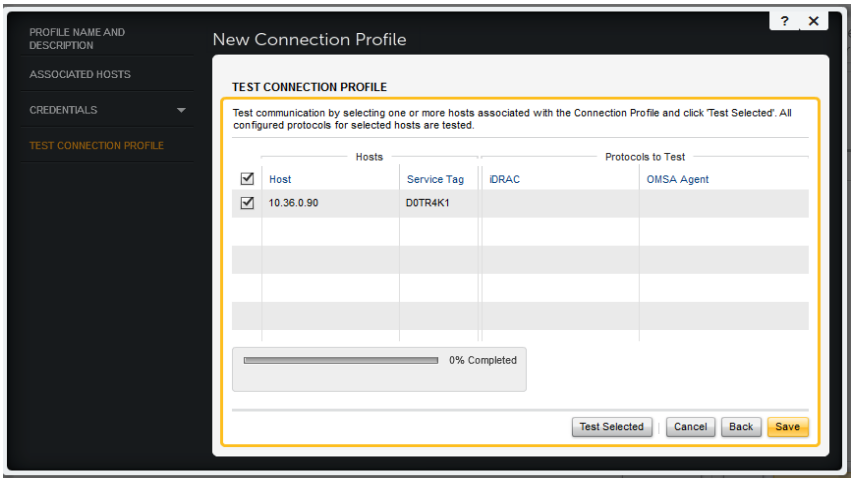
**Figure 2-10. Enter OMSA Agent Credentials**




7 On the **Test Connection Profile** page select one or more hosts associated with the connection profile, and click **Test Selected**. Click **Abort Tests** to cancel the test.

**NOTE:** For servers that do not have either an iDRAC Express or Enterprise card, the iDRAC test connection result will state **Not applicable for this system**.

**Figure 2-11. Test Connection**




8 Once the test completes, click **Save.**

9 To add connection profiles for additional hosts, repeat the previous steps.

10 When finished adding additional host, click **Save and Continue.**

## Events and Alarms

To select event posting options and enable, disable, or restore alarms:

1 Select the appropriate **Event Posting Level**.

- **Do not post any events** - Block hardware events.
- **Post All Events** - Post all hardware events.
- **Post only Critical and Warning Events** - Post only critical or warning-level hardware events.
- **Post only Virtualization-Related Critical and Warning Events** - Post only virtualization-related critical and warning events; this is the default event posting level.

2 Select the **Enable Alarms for Dell Hosts** check box to enable all hardware alarms and events.

3 Click **Restore Default Alarms** to restore the default vCenter alarm settings for all managed Dell servers; it may take up to a minute before the change takes effect.

4 Click **Save and Continue** to apply the changes and continue with the wizard.

**NOTE:** Dell hosts that have alarms enabled respond to critical events by entering maintenance mode. Click **Continue** to accept this change, or click **Cancel**.

### Proxy Settings

1 To use a proxy server, enter a DNS-resolved host name or IP address for **Proxy Server Address**. To not use a proxy server, skip to step 4.

2 Enter the **Proxy Port** number.

3 Select the **Credentials Required** check box, if needed. Enter a **Proxy User Name, Proxy Password**, and **Proxy Verify Password**.

4 Click **Save and Continue** to apply the changes and continue with the wizard.

### Schedule an Inventory Job

Within the configuration wizard on the **Inventory Schedule** page, enter the time to run the inventory weekly at a specific time and on selected days.

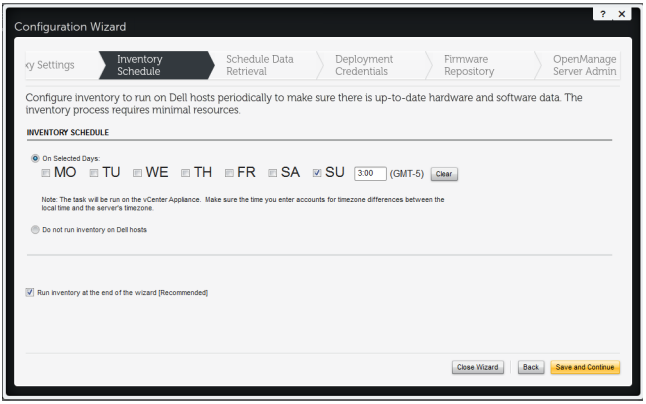
**NOTE:** It is recommended to schedule a weekly inventory job at minimum; otherwise, hardware information displayed in the Plug-in may be outdated. The inventory job consumes minimal resources and will not degrade host performance.

The inventory collects the hardware and status attributes including asset, server hardware, network, power monitoring, firmware identification, software applications, and storage information.

1 Select the **On Selected Days:** radio button, and then select the check box for the day of the week and enter the time. Click the **Clear** button to clear the entries.

2 Select the **Do not run inventory on Dell hosts** radio button to not run an inventory; this option is not recommended.

**Figure 2-12. Inventory schedule**


Configuration Wizard
Inventory Schedule
Schedule Data Retrieval
Deployment Credentials
Firmware Repository
OpenManage Server Admin
Configure inventory to run on Dell hosts periodically to make sure there is up-to-date hardware and software data. The inventory process requires minimal resources.
INVENTORY SCHEDULE
On Selected Days:
MO TU WE TH FR SA SU
3:00
(GMT-5)
Clear
Note: The task will be run on the vCenter Appliance. Make sure the time you enter accounts for timezone differences between the local time and the server's timezone.
Do not run inventory on Dell hosts
Run inventory at the end of the wizard [Recommended]
Close Wizard
Back
Save and Continue

3 Select the **Run inventory at the end of the wizard [Recommended]** check box to automatically run the inventory task once the wizard is complete.

4 Click **Save and Continue** to apply the changes and continue.

## Warranty Data Retrieval

Warranty settings control when warranty information is retrieved from Dell online by enabling or disabling the schedule and then setting a specific day and time to retrieve warranty updates.

1 Select the **On Selected Days** radio button to select the day and time for the warranty retrieval job.

2 Select the **Do not retrieve Warranty Data** radio button to not retrieve the data; this setting is not recommended.

3 Click **Save and Continue** to apply the changes and continue.

## Deployment Credentials

Deployment credentials are used to securely communicate with a bare-metal system, using the iDRAC6 from initial discovery until the end of the deployment process. Once deployment completes, the credentials are changed to those in the connection profile matched to the bare-metal system from the Deployment wizard.

If the deployment credentials are changed, all newly discovered systems from that point on will be provisioned with the new credentials; however, the credentials on servers discovered prior to the change are not affected.

The user name should be 16 characters or less (only ASCII printable characters).

The password should be 20 characters or less (only ASCII printable characters).

1. Enter **User name**.
2. Enter **Password**.
3. Enter **Verify Password**. Passwords must match.
4. Click **Save and Continue** to apply the changes and continue.

### Firmware Repository

Firmware repository settings contain the firmware catalog location used to update deployed servers. There are two location types:

- Dell online (ftp.dell.com) - Uses the default firmware update repository of Dell online (ftp.dell.com) with a required staging folder. The plug in will download selected firmware updates and store them in the staging folder, and then they are applied as necessary.
- Local/shared repository - Created with the Dell Repository Manager™ application. These local repositories should be located on Windows-based file shares.

To use Dell Online:

1. Select the **Dell online (ftp.dell.com)** radio button to use the Dell online repository location. Perform the following steps:
   a. Enter the **Staging Folder Location** using the following format:

      *host:/share* or *\\host\share*

      **NOTE:** When using a firmware repository on a network share, it must reside on a CIFS or NFS share that is accessible to the virtual appliance. Credentials are required for accessing CIFS share (to add domain to user name field if required.)

   b. If using a CIFS share for the staging folder, enter the **User Name, Password,** and **Verify Password**; the passwords must match. These fields are only active when entering a CIFS share.

c Click **Begin Test** to validate your entries.

2 Click **Save and Continue** to apply the changes and continue.

To use a local/shared repository:

1 Select the **Shared Network Folder** radio button to use a local/shared repository location. Perform the following steps:

a Enter the **Catalog File Location** using the following format:

```
host:/share/filename.xml,
host:/share/filename.gz,
\\host\share\filename.xml,
\\host\share\filename.gz
```

b If using a CIFS share, enter the **User Name, Password,** and **Verify Password**; the passwords must match. These fields are only active when entering a CIFS share

**NOTE:** The @ character is not supported for use in shared network folder user names/passwords.

c Click **Begin Test** to validate your entries.

2 Click **Save and Continue** to apply the changes and continue.

### OpenManage Server Administrator URL

Enter the OpenManage Server Administrator (OMSA) URL. The OMSA software can be used to:

- Manage vCenter elements (detailed sensor/component-level health information).
- Clear command logs and system event logs (SELs).
- Obtain NIC statistics.
- Make sure that the plug-in captures events from a selected host.

1 Enter the full URL including the *https* designation, and click **Finish**.

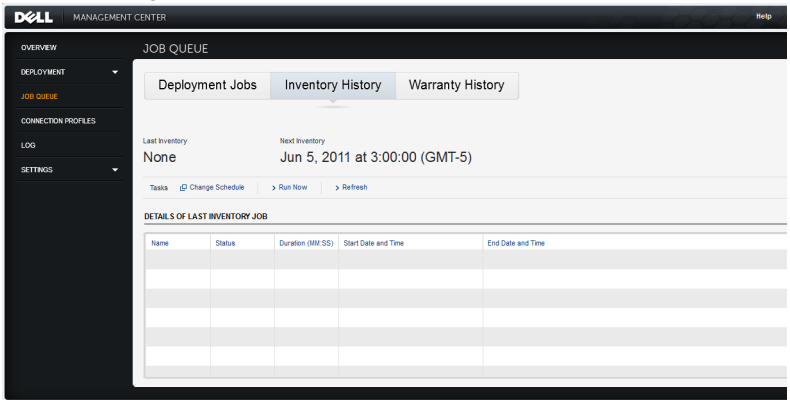
To launch OMSA within the Dell appliance, the OMSA Web Server must be installed and configured. See the *Dell OpenManage Server Administrator Installation Guide* for the version of OMSA in use for instructions on how to install and configure the Web Server.

## Immediately Run an Inventory

1 Once the configuration wizard is complete, click **Job Queue** –> **Inventory** –> **Run Now** to immediately run an inventory job.

2 Click **Refresh** to see the status of the inventory job.

**Figure 2-13. Job queue**




3 Navigate to the **Host and Cluster** view, click on any Dell host, then click the **Dell** tab. The following info should be available:

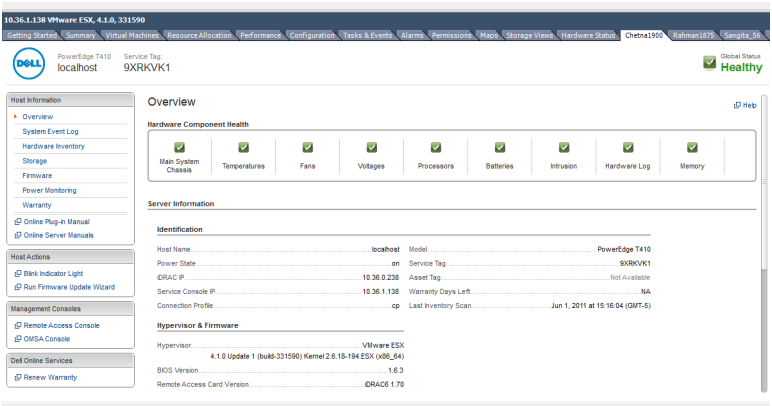
- Overview Page
- System Event Log
- Hardware Inventory
- Storage
- Firmware
- Power Monitoring
- Warranty Status

The following host commands will work within the **Dell** tab or by right-clicking on a host:

- Blink Indicator Light
- Run Firmware Update Wizard
- Launch Remote Access
- Launch OMSA

- Launch CMC
- Renew Warranty
- Proactive Systems Management

**Figure 2-14. Dell Tab in vSphere**




## Set Up an OMSA Trap Destination

1. Link and Launch the OMSA user interface, or navigate to the OMSA UI agent from a Web browser (https://<HostIP>:1311/).
2. Log in to the interface, and select the **Alert Management** tab.
3. Select the **Platform Events** option at the top of the tab.
4. Click the grey **Configure Destinations** button, and click the **Destination1** link.
5. Select the **Enable Destination** check box.
6. Enter the plug-in appliance IP address in the **Destination IP Address** field.
7. Click **Apply Changes**.

## Download Firmware Updates and Make Available

This functionality is only available for 11th generation Dell servers that have either an iDRAC Express or Enterprise card.

1 Download a Dell Update Package (DUP) executable file (.EXE) from **http://support.dell.com**.

2 Put the DUP on a Windows share drive that the vCenter host can access.

3 From **Dell** tab, select **Firmware –> Run Firmware Update Wizard**.

4 To use the **Load a single firmware update from a file** option:

   a Enter the file path in the following format:

   `\\<host accessible share path>\<FileName>.exe`

   b Enter the user name and password in a domain format that has access to the share drive.

   c Continue to step 7.

   Alternatively, to use the **Update from repository** option:

   a Select the **Update from repository** radio button.

   b Make sure you have a network connection to ftp.dell.com.

   c Click **Next**, and continue to step 5.

**Figure 2-15. Load a single firmware update from a file**

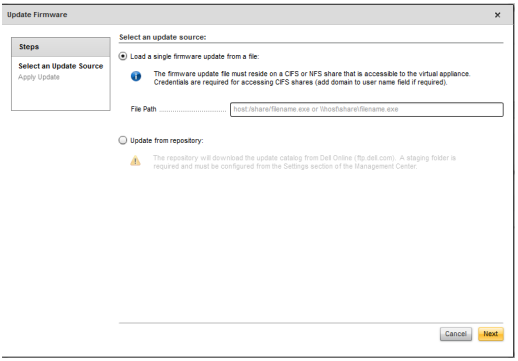
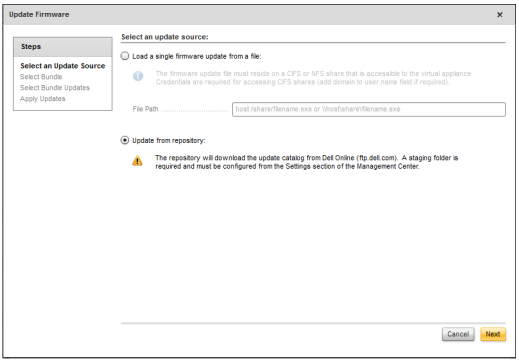
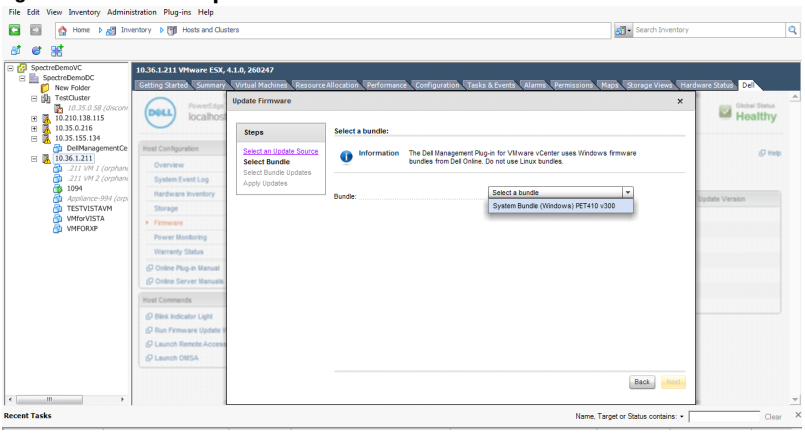

Update Firmware
Steps
Select an Update Source
Apply Update
Select an update source:
Load a single firmware update from a file:
The firmware update file must reside on a CIFS or NFS share that is accessible to the virtual appliance. Credentials are required for accessing CIFS shares (add domain to user name field if required).
File Path
host:/share/filename.exe or \\host\share\filename.exe
Update from repository:
The repository will download the update catalog from Dell Online (ftp.dell.com). A staging folder is required and must be configured from the Settings section of the Management Center.
Cancel
Next

**Figure 2-16. Update from repository**


Update Firmware
Steps
Select an Update Source
Select Bundle
Select Bundle Updates
Apply Updates
Select an update source:
Load a single firmware update from a file:
The firmware update file must reside on a CIFS or NFS share that is accessible to the virtual appliance. Credentials are required for accessing CIFS shares (add domain to user name field if required).
File Path
host:/share/filename.exe or \\host\share\filename.exe
Update from repository:
The repository will download the update catalog from Dell Online (ftp.dell.com). A staging folder is required and must be configured from the Settings section of the Management Center.
Cancel
Next

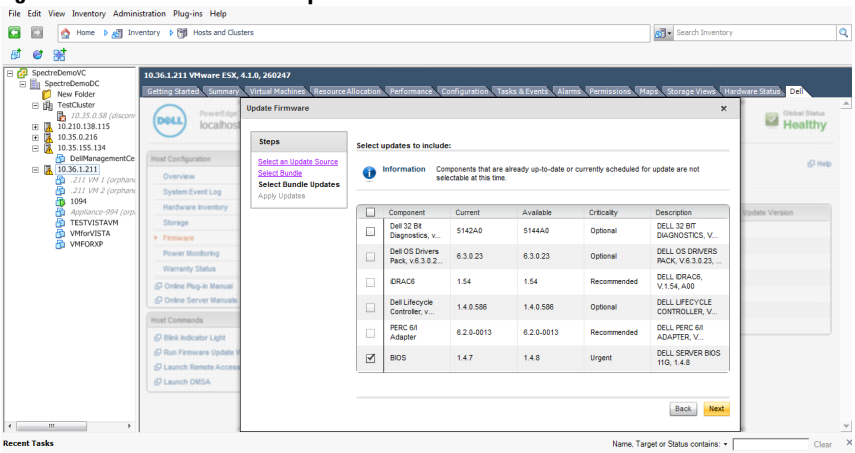
**5** Select the bundle for your host and click **Next**.

**Figure 2-17. Select update source bundle**




6 Select the desired firmware updates and click **Next**.

**Figure 2-18. Select firmware updates**

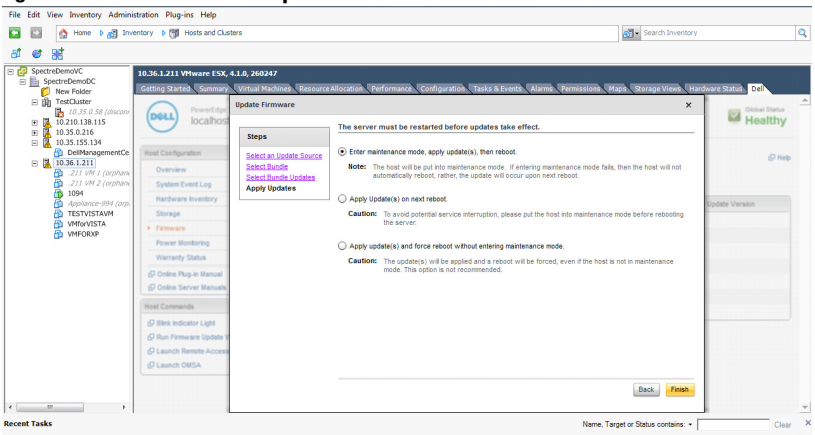



7 Select the desired restart option and click **Finish**:

- **Enter maintenance mode, apply updates, and restart** - Host goes into maintenance mode. If the host cannot enter maintenance mode, then the host is not restarted and the update is applied during the next reboot.

- **Apply updates on next reboot** - To avoid a service interruption, it is recommended that the host enters maintenance mode before the reboot.
- **Apply updates and force reboot without entering maintenance mode** - The update is applied, and a reboot occurs even if the host is not in maintenance mode. This method is not recommended.

**Figure 2-19. Select restart option and finish**


Update Firmware
The server must be restarted before updates take effect.
Steps
Select an Update Source
Select Bundle
Select Bundle Updates
Apply Updates
Enter maintenance mode, apply update(s), then reboot.
Note: The host will be put into maintenance mode. If entering maintenance mode fails, then the host will not automatically reboot, rather, the update will occur upon next reboot.
Apply Update(s) on next reboot.
Caution: To avoid potential service interruption, please put the host into maintenance mode before rebooting the server.
Apply update(s) and force reboot without entering maintenance mode.
Caution: The update(s) will be applied and a reboot will be forced, even if the host is not in maintenance mode. This option is not recommended.
Back
Finish
Recent Tasks

8 To verify that the update was successful, rerun the Inventory job using **Job Queue –> Run Now**, and review the Overview page to see the new versions.

## Configure Dell iDRAC Auto Discovery and Initial Start-up, and Disable/Enable User ID and Password

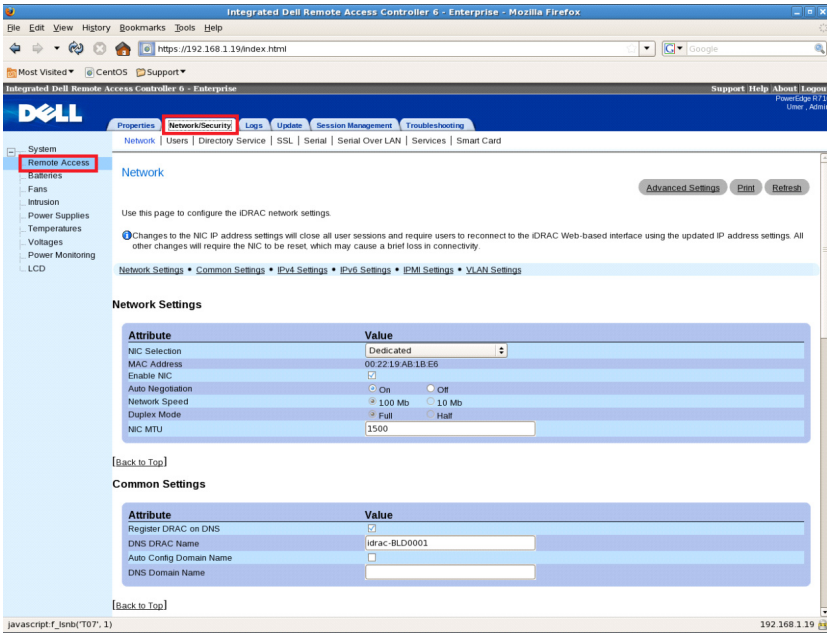
**NOTE:** For auto discovery and handshake to run, all users with admin-level access must be disabled. Additionally, if the deployment credentials in the appliance match those of an existing user, then the password of the existing user will be changed to match the appliance credentials.

1 Log in to the iDRAC user interface.

2 Click **Remote Access** in the left tree menu.

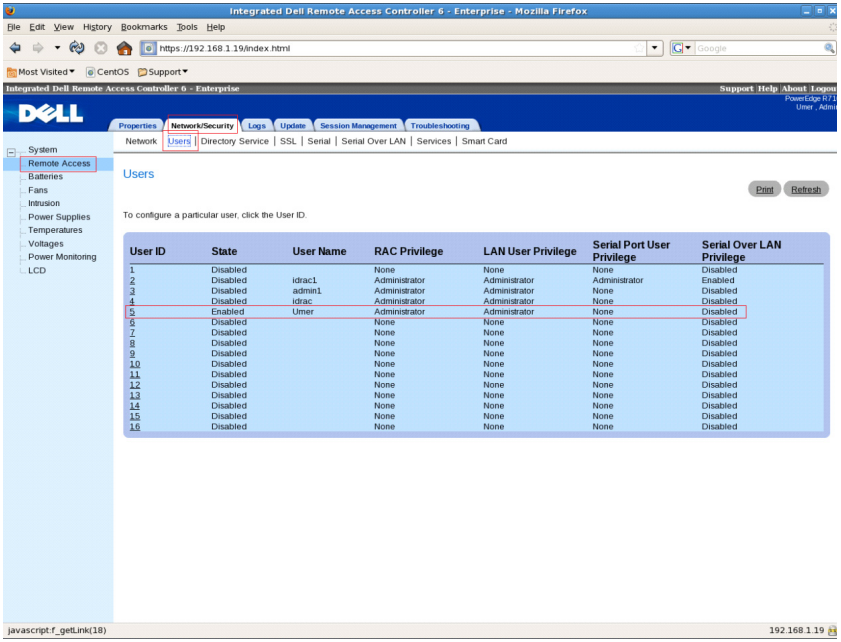
3 Click **Network/Security** in the main pane - upper tabs.

**Figure 2-20. Remote Access and Network/Security**



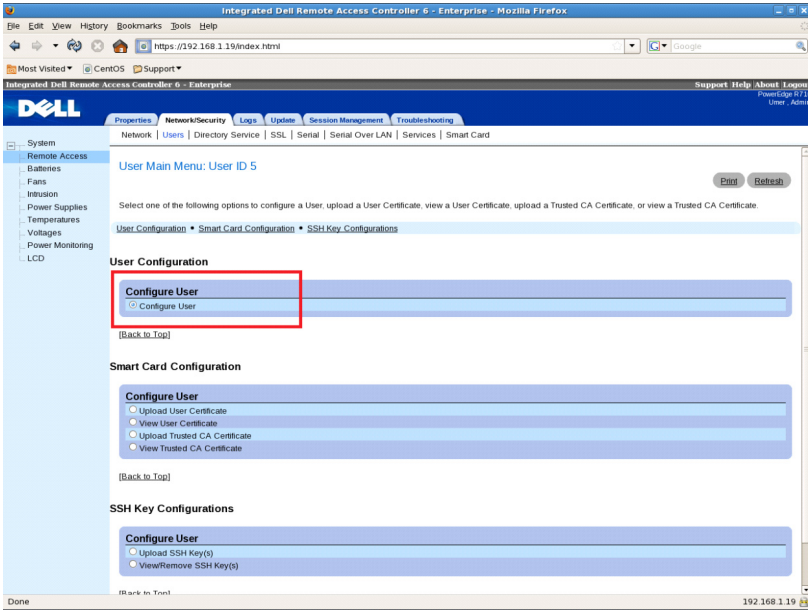

4 Click on the **Users** subtab, and select the user to edit by selecting the user ID link.

**Figure 2-21. Select a user to edit**


Integrated Dell Remote Access Controller 6 - Enterprise - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://192.168.1.19/index.html
Most Visited CentOS Support
Integrated Dell Remote Access Controller 6 - Enterprise
Support Help About Logout
Properties Network/Security Logs Update Session Management Troubleshooting
Network Users Directory Service SSL Serial Serial Over LAN Services Smart Card
System
Remote Access
Batteries
Fans
Intrusion
Power Supplies
Temperatures
Voltages
Power Monitoring
LCD
Users
Print Refresh
To configure a particular user, click the User ID.
User ID State User Name RAC Privilege LAN User Privilege Serial Port User Privilege Serial Over LAN Privilege
1 Disabled None None None Disabled
2 Disabled idrac1 Administrator Administrator Administrator Enabled
3 Disabled admin1 Administrator Administrator None Disabled
4 Disabled idrac Administrator Administrator None Disabled
5 Enabled Umer Administrator Administrator None Disabled
6 Disabled None None None Disabled
7 Disabled None None None Disabled
8 Disabled None None None Disabled
9 Disabled None None None Disabled
10 Disabled None None None Disabled
11 Disabled None None None Disabled
12 Disabled None None None Disabled
13 Disabled None None None Disabled
14 Disabled None None None Disabled
15 Disabled None None None Disabled
16 Disabled None None None Disabled
javascript:f_getLink(18)
192.168.1.19

5 Make sure that the **Configure User** radio button is selected, and continue to the next page.

**Figure 2-22. Configure user**


Integrated Dell Remote Access Controller 6 - Enterprise - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://192.168.1.19/index.html
Most Visited CentOS Support
Integrated Dell Remote Access Controller 6 - Enterprise
Support Help About Logout
DELL
Properties Network/Security Logs Update Session Management Troubleshooting
Network | Users | Directory Service | SSL | Serial | Serial Over LAN | Services | Smart Card
System
Remote Access
Batteries
Fans
Intrusion
Power Supplies
Temperatures
Voltages
Power Monitoring
LCD
User Main Menu: User ID 5
Print Refresh
Select one of the following options to configure a User, upload a User Certificate, view a User Certificate, upload a Trusted CA Certificate, or view a Trusted CA Certificate.
User Configuration • Smart Card Configuration • SSH Key Configurations
User Configuration
Configure User
Configure User
[Back to Top]
Smart Card Configuration
Configure User
Upload User Certificate
View User Certificate
Upload Trusted CA Certificate
View Trusted CA Certificate
[Back to Top]
SSH Key Configurations
Configure User
Upload SSH Key(s)
View/Remove SSH Key(s)
Done
192.168.1.19

6 To disable a user, uncheck the **Enable User** check box and click **Apply**. To enable a user, check the **Enable User** check box and click **Apply**.

7 Manually close the iDRAC user interface, then reboot the system and log back in.

8 When the system reboots, enter `ctrl-E` when the iDRAC IP address is displayed, and then go to **LAN USER CONFIGURATION** and set the **AutoDiscovery Flag** to **Enable**; make sure the iDRAC administrator accounts are disabled. Alternatively, to set up the network for auto discovery and handshake, refer to the *Dell Auto-Discovery Network Setup Specification* located at: **http://www.delltechcenter.com/page/Lifecycle+Controller**

9 Enter the plug-in appliance IP address in the **Provisioning server** field, and click enter and save to initiate discovery and initial start-up.

Installation and configuration is complete, and the Dell Management Plug-In is ready for use.

## NFS Share Configuration

To use NFS shares with the Management Plug-In for backup and restore operations, firmware updates and as a staging folder, there are certain configuration items that must be completed. CIFS shares do not require additional configuration.

1. Edit `/etc/exports` to add: `/share/path <appliance ip>(rw) *(ro)`

   This allows the virtual appliance full read and write access to the share, but limits all other users to read only.

2. Start nfs services:

   ```
   service portmap start

   service nfs start

   service nfslock status
   ```

   **NOTE:** The steps above may vary depending on the Linux distribution in use.

3. If any of the services were already running:

   ```
   exportfs -ra
   ```

## Uninstalling Dell Management Plug-In for VMware vCenter

To remove the Plug-in, it must be unregistered from the vCenter server using the Admin Portal:

1. Launch a browser window, and enter the **Admin Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

   **https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2. Click **VCENTER REGISTRATION** in the left pane. Click **Unregister** to unregister the Management Plug-in.

3. The Plug-in is now removed.

# Upgrading Dell Management Plug-In for VMware vCenter

There are four upgrade scenarios for the Dell Management Plug-In:

- "Upgrading from Version 1.0 to 1.0.1" on page 40
- "Upgrading from Trial Version 1.0.1 to Full Product Version 1.0.1" on page 41
- "Upgrading Dell Management Plug-in from 1.0.1 to 1.0.1 Update 1" on page 41
- "Upgrading Dell Management Plug-in using VCenter 5" on page 42

**NOTE:** Perform an appliance backup before you begin the upgrade. The backup can be performed using the Administration Console, see "Plug-in Database Backup and Restore" on page 85 for more information.

## Upgrading from Version 1.0 to 1.0.1

1. From the Administration Portal, select **VCENTER REGISTRATION - UNREGISTER** to unregister the 1.0 appliance version from any vCenter instances to which it is registered.
2. From the Administration Portal, select **BACKUP AND RESTORE** to backup the virtual appliance data to a network share location.
3. Shut down the 1.0 appliance from the vSphere client.
4. Deploy the new 1.0.1 appliance OVF from the vSphere client; set the administration password and configure networking through the appliance console user interface.

   **NOTE:** If the 1.0.1 appliance is using the same IP address as the 1.0 version, clear the Internet Explorer cache.
5. To upgrade to the 1.0.1 full product version, launch another browser window, and enter the **Admin Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

   **https://<ApplianceIPAddress>/DellAdminPortal/index.html**
6. The **Administration Console** login window displays. Enter the password and click **Login.**

7 There is a **Dell_Management_Center_license.bin** file included in the product download package. This file contains your product license, and must be uploaded to your appliance. To upload the license file, click **Upload License.**

8 On the **Upload License** window, click the **Browse** button to navigate to the license file. Click **Upload** to upload the license file.

9 Restore the 1.0 user data that was backed up from the network share to the 1.0.1 appliance using 1.0.1 Administration Portal.

10 Register the new 1.0.1 appliance to the vCenter instances.

11 Close and re-open any vSphere Client instances that are running, to reload the new security certificate used for 1.0.1 appliance communication.

12 After verifying the 1.0.1 appliance is functioning properly in your environment, you may remove the 1.0 appliance.

### Upgrading from Trial Version 1.0.1 to Full Product Version 1.0.1

1 Go to the Dell Web site and purchase the full product version.

2 The download will include the new full version product, and a new license file.

3 Launch another browser window, and enter the **Admin Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

**https://<ApplianceIPAddress>/DellAdminPortal/index.html**

4 The **Administration Console** login window displays. Enter the password and click **Login.**

5 There is a **Dell_Management_Center_license.bin** file included in the product download package. This file contains your product license, and must be uploaded to your appliance. To upload the license file, click **Upload License.**

6 On the **Upload License** window, click the **Browse** button to navigate to the license file. Click **Upload** to upload the license file.

### Upgrading Dell Management Plug-in from 1.0.1 to 1.0.1 Update 1

To upgrade to Dell Management Plug-in from 1.0.1 to 1.0.1. Update 1:

1 Launch a browser window, and enter the Admin Portal URL displayed in the **vSphere vCenter Console** tab for the virtual machine you want to configure or use the link from **Dell Management Console ->Settings** page. The URL uses the following format and is case sensitive:

   **https://<appliance IP address>**

   This navigates you correctly to the Admin Portal.

2 In the left pane of the **Admin Portal**, click **APPLIANCE MANAGEMENT**.

3 To upgrade do one of the following:

   - To use the default **Update Repository Path**, under **Appliance Settings**, click **Update Virtual Appliance**, and then skip to **step 7**.
   - To access the path to new downloaded RPMs, in the **Appliance Management** page, click **Edit**.

4 In the **Edit** group, in the **Update Repository Path** text box, enter the path for the location of the RPMs for 1.0.1 Update 1.

5 To save this change, click **Apply**.

6 To to apply the update to the virtual appliance, under **Appliance Settings**, click **Update Virtual Appliance**.

7 In the **Update Appliance** dialog box, click **Upgrade**. Once you click Upgrade you are logged off the Administrator Portal.

### Upgrading Dell Management Plug-in using VCenter 5

Dell Management Plug-in version 1.0.1 does not support VCenter 5. If using a vCenter 5 only environment the Plug-in must be updated to 1.0.1 Update 1. Doing the order other than the following procedure causes the Events not to appear correctly in VCenter 5 at the Host and DataCenter level.

**NOTE:** Use these steps only if your environment is exclusively vCenter 5. If in a mixed environment, then update the to Dell Management Plug-in 1.0.1 Update, see "Upgrading Dell Management Plug-in from 1.0.1 to 1.0.1 Update 1" on page 41. If you are using an older vCenter Server, then register your vCenter 5, and only use steps 1, 2, and 3.

To upgrade Dell Management Plug-in using vCenter 5:

1 Launch a browser window, and enter the Admin Portal URL displayed in the **vSphere vCenter Console** tab for the virtual machine you want to configure or use the link from **Dell Management Console ->Settings** page. The URL uses the following format and is case sensitive:

**https://<appliance IP address>**

This navigates you correctly to the Administration Portal.

2 Do one of the following:

- If your network requires a proxy server to access the network, in the **vCenter Registration page**, register the Dell Management Plug-in by clicking **Register New vCenter Server**.
- If no proxy is required, skip to step 6.

3 In the **Register New vCenter** dialog box do the following:

- Under **vCenter Name**, in the **vCenter Server IP or Hostname** text box, enter the IP or hostname of the vCenter server.
- In the **Description** text box, enter an optional Description.
- Under **Admin User Account**, in the **Admin User Name** text box type the Admin user name.
- In the **Password** text box, type the password.
- In the **Verify Password** text box, re-type password.
- Click **Register**.
- Go to **vCenter** and verify the Dell Management Plug-in shows up.

4 In **vCenter -> Dell Management Center -> Settings**, set up your Proxy, see "Proxy Settings" on page 55.

5 Return to the Administrative Portal to Update the virtual appliance.

6 In the left pane of the **Admin Portal**, click **APPLIANCE MANAGEMENT**.

7 To upgrade do one of the following:

- To use the default **Update Repository Path**, under **Appliance Settings**, click **Update Virtual Appliance**, and then skip to **step 10**.
- To access the path to new downloaded RPMs, in the **Appliance Management** page, click **Edit**.

8 In the **Edit** group, in the **Update Repository Path** text box, enter the path for the location of the RPMs for 1.0.1 Update 1.

9 To save this change, click **Apply**.

10 To to apply the update to the virtual appliance, under **Appliance Settings**, click **Update Virtual Appliance**.

11 In the **Update Appliance** dialog box, click **Upgrade**. Once you click Upgrade you are logged off the Administrator Portal.

12 Once the update completes and the virtual appliance is back up, choose one of the following:

- If a proxy was used, then unregister the Dell Management Plug-in and re-register the it again by continuing to step 13. Not un-registering and re-registering causes Events not to appear correctly in VCenter 5 at the Host and DataCenter level.
- If a proxy was not used and a vCenter 5 was never registered, then complete step 1, 2 and 3 to register a new vCenter 5 server.

13 To unregister,, open the Admin Portal (step 1) and go to the **vCenter Registration** page, in the vCenter Server table that lists the servers, click **Unregister.**

14 Re-register following the directions in step 3.

# 3

# End-to-End Hardware Management

The goal of end-to-end hardware management is to provide the system health status and up-to-date infrastructure information that an administrator needs to respond to critical hardware events without leaving the management center or vCenter. End-to-end hardware management within the Management Plug-In is broken down into four separate parts: monitoring, inventory, advanced host management, and warranty retrieval.

## Monitoring

Datacenter and host system monitoring allows an administrator to monitor infrastructure health by displaying hardware (server and storage) and virtualization-related events on the **Tasks & Events** tab in vCenter. Additionally, critical hardware alarms can trigger the plug-in to put the host system into a maintenance mode, and in certain cases migrate the virtual machines to another host system. The Dell Plug-In forwards OMSA alarms, and creates new ones for specific events. These alarms can then be used to trigger actions that vCenter allows, like a reboot, maintenance mode, or migrate. For examples, when a dual power supply fails and an alarm is created, the resulting action can be to migrate the VM on that machine to a new one.

To perform monitoring:

1. Configure the **Event and Alarm** settings
2. Configure OMSA trap destinations, if needed.
3. Use the **Tasks&Events** tab in vCenter to review event information

### Configure Event and Alarm Settings

To select event posting options and enable, disable, or restore alarms:

1. From the management center, select **Settings - Events and Alarms**.
2. Click **Edit** to display the configuration options.
3. Select the appropriate **Event Posting Level**:
   - **Do not post any Events** - Block hardware events.
   - **Post All Events** - Post all hardware events.

- **Post only Critical and Warning Events** - Post only critical or warning-level hardware events.
- **Post only Virtualization-Related Critical and Warning Events** - Post only virtualization-related critical and warning events; this is the default event posting level. See *Appendix A: Virtualization-Related Events* for more information.

**NOTE:** A critical event indicates actual or imminent data loss or system malfunction, and a warning event is not necessarily significant, but may indicate a possible future problem.

4 Select the **Enable Alarms for Dell Hosts** check box to enable all hardware alarms and events. In response to certain alarms and events, the plug-in will:

   a Put the host into maintenance mode and migrate all of the workloads off of the server in response to **critical hardware events.**

   b Put the host into maintenance mode only in response to **less critical hardware events.**

   A pop-up window is displayed that states that any hosts that are outside of clusters, or do not have the Distributed Resource Scheduler (DRS) enabled could have virtual machines shut down during a critical event; the impacted servers are listed in the table. Click **Continue** to accept this change, or click **Cancel**.

5 Click **Restore Default Alarms** to restore the default vCenter alarm settings for all managed Dell servers.

6 Click **Save** to apply changes, or click **Cancel** to retain previous settings.

### Set up an OMSA trap destination

This task should only be completed for host systems utilizing OMSA for event generation instead of iDRAC6; there is no additional configuration required for iDRAC6.

1 Either use the link to the OMSA user interface found in **Settings - General**, or navigate to the OMSA agent from a Web browser (https://<HostIP>:1311/).

2 Log in to the interface, and select the **Alert Management** tab.

3. Select **Alert Actions** and make sure that any events to be monitored have the **Broadcast Message** option set, so that the events will be sent out.
4. Select the **Platform Events** option at the top of the tab.
5. Click the grey **Configure Destinations** button, and click the **Destination1** link.
6. Select the **Enable Destination** check box.
7. Enter the plug-in appliance IP address in the **Destination IP Address** field.
8. Click **Apply Changes**.
9. Repeat step 1 to step 8 to configure additional events.

### View Events

To view events, either navigate to the vCenter **Tasks&Events** tab and select the **Events** view so that the selected level of events is displayed, or click on the parent node (cluster or datacenter) of the host or the root folder of the vCenter. Events will appear only on those nodes in the vSphere tree.

## Inventory

Datacenter and host system inventory allows an administrator to view the current hardware configuration and status information for an individual or group of host systems. The information displayed includes:

- Asset information
- Server inventory
- Networking
- Overall global health
- Storage inventory
- Firmware inventory

An inventory of all host systems must be collected to display this information. To perform an inventory on host systems, a connection profile that provides communication and authentication information must be created. Once the inventory is complete, the inventory results can be viewed for the entire datacenter or for an individual host system.

To perform host system inventory:

1. Create a **Connection Profile**.
2. Schedule and run an **Inventory Job** on all host systems.
3. Use either the individual host tab or see the datacenter/cluster/folder level to view datacenter or host system component-level status and information.
4. Use the **Recent Tasks** window below the individual host tab view to view system event log information for all inventoried host systems. If an inventory job has failed, the reason for the failure is also listed.

### Managing Connection Profiles

Connection Profiles associate access and deployment credentials with a set of host systems and typically contain:

- Name and unique description (to help with profile management)
- A list of hosts associated with the connection profile
- iDRAC credentials
- OMSA agent credentials

To add a new connection profile:

1. From the management center, select **Connection Profiles.**
2. Under **Available Profiles,** click **Create New**. The **New Connection Profile** pop-up displays.
3. Enter the **Profile Name** and an optional **Description** that can be used to help manage custom connection profiles, and click **Next**. To stop adding a new profile, click **Cancel**, or to return to a previous section, click **Back**.
4. For **Associated Hosts**, select the hosts that will use the connection profile and click **Next**.
5. View the information about credentials and connection protocols and click **Next**.
6. Enter the **iDRAC** credential information and click **Next**:
   a. **User Name**, **Password**, and **Verify Password;** the passwords must match and use ASCII-printable characters only. See the **Credentials** section of "Create and Assign Connection Profiles" on page 21 for more information.

   **NOTE:** Passwords cannot exceed 20 characters.

b For **Certificate Check**, select **Enable** to download and store the iDRAC certificate and validate it during all future connections, or select **Disable** to perform no check and not store the certificate.

7 Enter the in-band **OMSA agent** credential information and click **Next**:

a **User Name**, **Password**, and **Verify Password**; the passwords must match.

**NOTE:** Passwords cannot exceed 31 characters.

**NOTE:** The OMSA credentials are the same credentials used for ESX and ESXi hosts.

b For **Certificate Check**, select **Enable** to download and store the OMSA certificate and validate it during all future connections, or select **Disable** to perform no check and not store the certificate.

8 The **Test Connection** window tests the entered iDRAC and OMSA agent credentials on the selected servers. Click **Test Selected** to begin the test; the other options are inactive. To stop the tests click **Abort Tests.**

9 Click **Save** to complete the profile.

To view or edit an existing connection profile:

1 From the management center, select **Connection Profiles.**

2 Select the profile to edit and click **Edit/View**.

3 The **Connection Profile: Profile name** window displays.

4 Select the profile section to edit/view, and make the appropriate changes:

- **Profile Name and Description:** Rename profile or change description
- **Associated Hosts:** Hosts using connection profiles

**NOTE:** When an existing server is added to a connection profile, an Inventory Job must be manually run to update the management center with the new server's information.

- **iDRAC credentials:** User name, password, and certificate check
- **OMSA agent credentials:** User name, password, and certificate check

5 Click **Save** to apply changes, or click **Cancel** to eliminate changes.

6 Click **X** (upper-right corner) to close the window.

To delete a connection profile:

1 Select a profile and click **Delete**; a message is displayed.

2 Click **Delete** on the message box to remove the profile, or click **Cancel** to cancel the delete action.

To test a connection profile:

1 Click **Test Connection** to test the entered iDRAC and OMSA agent credentials on the selected servers. Click **Test Selected** to being the test, and click **Abort All Selected** to cancel the testing.

To refresh the connection profiles:

Click **Refresh**.

**NOTE:** If a host is removed from vCenter, then it is removed from the connection profile.

### Schedule and Run Inventory

The **Inventory Schedule** sets the time/day for running inventory jobs, such as:

- Weekly at a specific time and on selected days
- At a set time interval

A completed inventory is **required** to gather the data needed by the majority of the Management Plug-In features.

**NOTE:** To make sure that the inventory contains up-to-date information, the inventory job should run a minimum of once a week. The inventory job consumes minimal resources and does not degrade host performance.

To modify the inventory job schedule:

1 From the management center, select **Settings - Inventory Schedule**.

2 Click **Edit** to change the current schedule.

3 Select the **On Selected Days:** radio button, and then select the check box for the day of the week and enter the time. Click the **Clear** button to clear the entries.

4 Click **Apply** to change the inventory schedule, or click **Cancel** to cancel.

5 From the management center, select **Job Queue** and the **Inventory History** tab.

6 Click **Run Now** to immediately run the inventory job.

7 To update the **Details of Last Inventory Job,** click **Refresh**.

### Display Server Hardware Configuration and Status

Once the inventory job completes, to view the inventory for an entire datacenter:

1. From the vSphere client, under the **Inventory** heading select **Hosts and Clusters.**
2. From **Hosts and Clusters**, select the datacenter in the tree view and select the Management Plug-In tab.
3. An **Overview** of all hosts in the datacenter is displayed. Use the **View** drop-down to view an inventory category:
   - Hardware: Field Replaceable Units
   - Hardware: Processors
   - Hardware: Memory
   - Hardware: NICs
   - Hardware: PCI Slots
   - Hardware: Remote Access Card
   - Storage: Physical Disks
   - Storage: Virtual Disks
   - Firmware
   - Power Monitoring
   - Warranty
4. Use the *Filter* text box to enter a filter for the inventory data.
5. Click **Refresh** to refresh the displayed inventory.
6. Click **Export** to export the inventory as a CSV file. A download location window is displayed; select the location to save the inventory and click **Save.**

To view the inventory for a single host system:

1. From the vSphere client, under the **Inventory** heading select **Hosts and Clusters.**
2. From **Hosts and Clusters**, select the host system in the tree view and select the Management Plug-In tab.
3. An **Overview** of the selected host is displayed.

The Overview provides information on key host server attributes, including individual component health, identification, hypervisor, and firmware information.

- **Component Health** is a graphical representation of the status of all major host server components: system chassis, power supply, temperature, fans, voltage, processors, batteries, intrusion, hardware log, power management, and memory. The available status states are:
  - Healthy (green check mark) - component operating normally
  - Warning (yellow triangle with exclamation point) - component has a non-critical error
  - Critical (red X) - component has a critical failure
  - Unknown (question mark) - status is unknown for the component

  A global health status is displayed in the upper-right header bar.
- **Server Information** provides **Identification**, **Hypervisor, and Firmware** information, such as:
  - Host name, power state, iDRAC IP address, console IP address, connection profile in use, model, service tag and asset tag numbers, number of days left on the warranty, and when the last inventory scan was performed
  - Hypervisor, BIOS firmware, and iDRAC firmware versions
- **Recent System Log Entries** provide the 10 most recent system event log entries. Click **Details** to launch the **System Event Log** window that displays additional log details.

4 Select **Hardware Inventory** to display a list and further details on all components installed in host system, including:

- Field-replaceable units (FRUs) - DIMMS, system planar, power supplies, backplanes, controller cards, etc.
- Memory - Number of slots available and in use, maximum capacity and amount of memory in use, and details on individual DIMMs.
- Network Interface Cards (NICs) - Number of installed cards and details on individual NICs.
- PCI Slots - Total available and number in use, and details on individual slots.

- Power Supplies - Number present and details on individual PSUs.
- Processors - Number present and details on individual CPUs.
- Remote Access Card - IP address information, RAC type, and Web interface URL.

5 Select **Storage** to display a graphic and detailed view of the capacity and type of physical and virtual storage, including:
- Host system total storage, unconfigured, configured, and global hot spare disk capacity.
- List of how many of each storage component is present in the system.
- Component data table that contains detailed information on that component.

6 Select **Firmware** to display all Dell Lifecycle Controller firmware information including:
- Update name - BIOS, Dell Lifecycle Controller, power supply, etc.
- Update type - BIOS, firmware, or application.
- Individual update details - Version, installation time, if an update is in progress or the update status, and the update version. The update status and version only have data when an update is scheduled, and the update version is the firmware version to which the system will be updated.

7 Select **Power Monitoring** to display general power information, energy statistics, and reserve power information, including:
- Current power budget, profile, warning and failure thresholds
- Energy consumption, system peak power, and amperage statistics
- Reserve power and peak reserve capacity

8 Select **Warranty Status** to display system warranty information including:
- Warranty provider name and description of the warranty
- Start and end dates and how many days are left on the warranty
- Status of the warranty (active, inactive) and when the warranty information was last updated

### Display System Event Logs

System Event Logs provide information based on the following criteria:

- Status - Info (blue exclamation point), Warning (yellow triangle with exclamation point), Error (red X)
- Time (Server Time)- time and date the event occurred
- Search text - specific message, server names, configuration settings, etc.

The severity levels are defined as:

- **Info:** The Management Plug-In operation completed successfully.
- **Warning**: The Management Plug-In operation partially failed, and was partially successful.
- **Error**: The Management Plug-In operation failed.

The log can be saved as an external CSV file.

To display the System Event Logs for all host systems:

1. From the management center, select **Logs.**
2. Click **Refresh** to update the log with the most recent data.
3. Click the **All Categories** drop-down menu to select a severity category to filter the log data: All Categories, Info, Warning, Error, or Security.
4. Click the **Last Week** drop-down menu to select a data range to filter the log data: Last week, Last Month, Last Year, or Custom Range.

   If Custom Range is selected, **Start Date** and **Stop Date** drop-down menus are displayed. To set the customer date range:

   a. Click the calendar wizard to populate the **Start** date.

   b. Click the calendar wizard to populate **End** date.

   c. Click **Apply**.
5. To control how the log is displayed, use the display controls to set the **Records per screen,** go to a desired **Page**, and use the forward and backward page controls.
6. To export the entire Log contents to a comma-separated value (CSV) file, click **Export**. A download location window is displayed; select the location to save the log and click **Save.**

To display the System Event Logs for an individual host system:

1. From the vSphere client, under the **Inventory** heading select **Hosts and Clusters.**
2. From **Hosts and Clusters**, select the host system in the tree view and select the Management Plug-In tab. An **Overview** of the selected host is displayed.
3. From **Recent System Log Entries** click **Details** to launch the **System Event Log** window that displays the System Event Log.
4. To update the System Event Log to make sure all of the latest entries are displayed, click **Refresh Log**.
5. To limit (filter) the number of event log entries:
   a. Select the **Search Filter** text box, and enter a text string to dynamically filter the log entries.
   b. Click X to clear the filter text box, and all event log entries will be displayed.
6. To clear all event log entries, click **Clear Log**. A pop-up message displays stating that all log entries are deleted after they are cleared. Click **OK** to clear the log entries, or click **Cancel** to cancel.
7. To export the event log to a CSV file, click **Export**. A download location window is displayed; select the location to save the system event log and click **Save.**

# Advanced Host Management

The advanced host management tasks are host system-based actions that allow an administrator to identify a physical server in the datacenter environment, launch server-based management tools, and display server warranty information. All of these actions are initiated from the Management Plug-In tab for an individual host system.

### Server Identification

To assist in locating a physical server in a large physical datacenter environment, the front indicator light can blink for a set time period.

1. From the vSphere client, under the **Inventory** heading select **Hosts and Clusters.**

2 From **Hosts and Clusters**, select the host system in the tree view and select the Management Plug-In tab.

3 Under **Host Commands**, select **Blink Indicator Light**.

4 Select **Blink On**, and use the **Timout** drop-down menu to set the time period. Click **OK** to cause the light to start blinking.

5 To stop the light from continuing to blink, select **Blink Off** and click **OK**.

### Server-Based Management Tools

There are two server-based management tools, iDRAC6/DRAC and OMSA, that can be launched from the Management Plug-In tab.

- Click **Launch Remote Access** to launch the iDRAC 6 user interface.
- Click **Launch OMSA** to launch the OpenManage Server Administrator user interface URL that was entered into the management center either during the initial configuration wizard or using **Settings –> General**. The URL is for the server administrator Web server, and must be installed on a Windows-based management station.
- Click **Launch CMC** to launch the Chassis Management Controller user interface.

### Proactive Systems Management

Proactive Systems Management is a free remote-support software that can be used to:

- Monitor potential hardware failures
- Alert you of potential problems within five minutes of detection
- Help uncover and analyze problems with automated diagnostics
- Provide proactive dispatch of qualified parts, direct from Dell
- Help accelerate resolution by automatically generating a support case when a hardware fault is detected
- Provide advanced notification of upcoming service contract expirations
- Provide a consolidated view of the IT environment
- Allow corrective action to be taken to minimize downtime

This software is a separate service that must be installed and configured outside of the Plug-In.

To display Proactive Systems Management links in the hosts view:

1. From the management console, select **Settings - General**.
2. Under **Proactive Systems Management**, click **Edit.**
3. Select the **Show Proactive Systems Management login page in the Hosts view** check box. Click **Apply.**
4. A link to the Proactive Systems Management portal and one for a Learn More Web site that contains additional details about the software are displayed under **Proactive Systems Management**.

# Warranty Retrieval

Warranty retrieval provides the following information for Dell servers:

- Updated service warranty information, while only transmitting the host service tag
- Warranty information updated at scheduled intervals
- Secure transmission using a proxy server and credentials
- Information through a tested, secure connection

**NOTE:** The service tag information transmitted to Dell online is not stored.

To enable the warranty retrieval schedule:

1. Select **Warranty Schedule** under **Settings**, and click **Edit**.
2. Select the **On Selected Days** radio button to select the day and time for the warranty retrieval job.
3. Click **Apply** to change the warranty update schedule.
4. From the management center, select **Job Queue** and the **Warranty History** tab.
5. Click **Run Now** to immediately run the warranty retrieval job.
6. To update the **Details of Last Warrant Job,** click **Refresh**.

### Display Server Warranty Information

Once the warranty job completes, to view the warranty information for an entire datacenter:

1. From the vSphere client, under the **Inventory** heading select **Hosts and Clusters.**
2. From **Hosts and Clusters**, select the datacenter in the tree view and select the Management Plug-In tab.
3. An **Overview** of all hosts in the datacenter is displayed. Use the **View** drop-down to select **Warranty**.
4. In the **Filter** text box, enter a filter for the warranty data.
5. Click **Refresh** to refresh the displayed inventory.
6. Click **Export** to export the inventory as a CSV file. A download location window is displayed; select the location to save the inventory and click **Save.**

To view the warranty information for a single host system:

1. From the vSphere client, under the **Inventory** heading select **Hosts and Clusters.**
2. From **Hosts and Clusters**, select the host system in the tree view and select the Management Plug-In tab.
3. Select **Warranty Status** to display system warranty information including:
   - Warranty provider name and description of the warranty
   - The start and end dates and how many days are left on the warranty
   - The status of the warranty (active, inactive) and when the warranty information was last updated

### Proxy Settings

The proxy settings define the HTTP proxy and any required credentials used to retrieve information from the Web (including from Dell online), such as:

- Enable or disable the proxy server
- Enter the **Proxy Server** and **Port Number** needed
- Define any required credentials - **User name** and **Password**

**NOTE:** Proxy passwords cannot exceed 31 characters.

To configure the HTTP proxy:

1. Select **Proxy** under **Settings**, and click **Edit**.
2. Enter a DNS-resolved host name or IP address for **Proxy Server Address**.

3 Enter the **Proxy Port** number.

4 Select the **Credentials Required** check box, if needed. Enter a **Proxy User Name, Proxy Password,** and **Proxy Verify Password**.

5 Click **Apply** to save the new settings.

To use the HTTP proxy when retrieving Web-based data:

1 Select the **Use Proxy** check box.

2 Click **Test Connection** to validate settings.

3 Click **Apply**.

# 4

# Zero-Touch Hardware Provisioning and Deployment

## Hardware Prerequisites

To successfully perform hardware provisioning and deployment, the physical servers must appear in the Deployment Wizard. All physical servers must meet the following prerequisites:

1. The server must be an 11G server. See the *Dell Management Plug-In for VMWare vCenter Version 1.0.1 Release Notes* for specific hardware support information.
2. The server must have the minimum supported versions of iDRAC firmware, Lifecycle controller and BIOS. See the *Dell Management Plug-In for VMWare vCenter Version 1.0.1 Release Notes* for specific hardware support information.

   **NOTE:** If the firmware versions are older, there could be a two step process to upgrade to the minimum required versions. See the firmware documentation for detailed upgrade instructions.
3. If using add-on NICs, the system must have the host LOMs enabled; the Plug-in allows deployment only onto a host LOM. The management NIC can be changed manually, and the system then added to vCenter.
4. If the iDRAC is in dedicated mode, its NIC must be enabled and the iDRAC should be able to communicate with the Plug-in.
5. CSIOR must be enabled, and a cold reboot performed on the system before initiating Auto Discovery to make sure that the retrieved data is current. A cold reboot requires that power is removed from the system, wait for a complete shut down of all components, and then reapply power. See "Setting Collect System Inventory on Restart (CSIOR) on a Clone Server" on page 65 for information on how to enable CSIOR.
6. To enable Auto Discovery and handshake, a server can be ordered with deployment and hardware provisioning enabled from the factory. The provisioning server Plug-in IP address information is either entered

manually, or the network can be configured to provide this information. For the manual setup instructions, see "Configure Dell iDRAC Auto Discovery and Initial Start-up, and Disable/Enable User ID and Password" on page 36 for more information. For network configuration instructions, see "Enabling Auto-Discovery on a Newly-Purchased System" on page 99 for more information.

7 If the Plug-in is not used for hardware configuration, then make sure the following conditions are met prior to initiating hypervisor deployment:

- BIOS configuration needs to be set to change the **VT** flag to Enabled.
- The system needs to have a Virtual Disk for installation of the OS. The Plug-in will not install the hypervisor to an internal SD card.

8 If the Plug-in is used for hardware configuration, the BIOS setting for VT is automatically enabled, even if BIOS configuration is not part of the hardware profile. Express/Clone RAID configuration will be required if a virtual disk is not already present on the target system.

9 The deployment process installs the OpenManage Server Administrator package on the target system, and will automatically configure the SNMP trap destination to point to the Dell Plug-in.

# Overview

Once a physical inventory of the datacenter is complete, all auto-discovered bare-metal systems are available to the Management Plug-in for zero touch hardware provisioning and hypervisor deployment. To prepare for provisioning and deployment, you must:

1 Create a Hardware Profile - Contains the hardware settings gathered from a *reference server* that will be used to deploy new servers.

2 Create a Hypervisor Profile - Contains the hypervisor installation information needed for ESX/ESXi deployment.

3 Create a Deployment Template - Optionally contains a hardware profile, a hypervisor profile, or both; can be saved and reused as needed for all available datacenter servers.

Once the deployment template is created, the **Deployment Wizard** can be used to gather the information necessary to create a scheduled job that provisions server hardware and deploys new hosts in vCenter. Lastly, the **Job Queue** can be used to view job status and make changes to pending deployment jobs.

## Understanding Deployment Job Times

Provisioning and deploying bare-metal servers can take between 30 minutes and a couple of hours to complete, depending on certain factors. When starting a deployment job, it is recommended that you plan your deployment time according to the guidelines provided.

The amount of time it takes to complete provisioning and deployment varies with deployment type, complexity, and number of deployment jobs running simultaneously. Table 4-1 gives you guidelines of the approximate time a deployment job may take.

Deployment jobs are run in batches of up to five concurrent servers, to improve time for the overall deployment job. The exact number of concurrent jobs depends on resources available.

**Table 4-1. Approximate Deployment Time Scenarios**

| Deployment Type | Approximate Time Per Deployment |
|---|---|
| Hypervisor only | Between 30 minutes to 1 hour. |
| Hardware only | Up to 2 hours depending on the complexity and the RAID, BIOS, and boot options to configure |
| Hypervisor and Hardware profiles | 1 to 4 hours |

## Server States Within the Deployment Sequence

When an inventory job is run, auto-discovered bare-metal systems are classified in different states to help determine if the server is new to the datacenter or has a pending deployment job scheduled. Administrators can use these states to determine if a server should be included in a deployment job. The states are:

- Unconfigured - The server has contacted the Management Plug-In and is waiting to be configured.

- Configured - The server is configured with all hardware information required for a successful hypervisor deployment.

## Configure a Hardware Profile

To configure server hardware settings, a hardware profile must be created. A hardware profile requires the following information:

- Boot Order - Boot device sequence, hard drive sequence, which can be edited only if the boot mode is set to BIOS
- BIOS Settings - Memory, processor, SATA, integrated devices, serial communications, embedded server management, power management, system security, and miscellaneous settings
- iDRAC Settings - Network, user list, and user configuration (IPMI/iDRAC privileges)

  **NOTE:** For systems that have iDRAC Express, the iDRAC configuration cannot be extracted; therefore, the server should not be used as a reference server. If it is used as a target system, then no iDRAC configuration from the reference server will be applied.
- RAID Configuration - Displays the current RAID topology on the reference server at the time the hardware profile was extracted.

  **NOTE:** If using the **Customize settings from reference server** option in the hardware profile, the RAID configuration task defaults to RAID1 on the first two drives of the integrated controller that are RAID1 capable. Additionally, a dedicated hot-spare for the RAID1 array is created if a candidate drive meeting the criteria exists.

  **NOTE:** The Management Plug-In enables certain BIOS settings under the Processor group in the BIOS on all deployed servers, regardless of the settings on the reference server. Before using a reference server to create a new hardware profile, it must have the Collect System Inventory On Restart (CSIOR) setting enabled and be restarted to provide accurate inventory and configuration information. See below for more information.

### Setting Collect System Inventory on Restart (CSIOR) on a Clone Server

There are two methods for setting CSIOR: Locally on an individual host using the Dell Lifecycle Controller United Server Configurator (USC) user interface or remotely using a WS-Man script. For more information on scripting this functionality, see the *Dell Tech Center* and the *DCIM Lifecycle Controller Management Profile*.

To enable CSIOR locally on a reference server:

1. Power on the system, and during POST press <F10> to launch USC.
2. Select **Hardware Configuration - Part Replacement Configuration.**
3. Enable the **Collect System Inventory on Restart** setting, and exit USC.

### Create New Hardware Profile

To create a new hardware profile, an administrator enters reference server hardware configuration information. There are two ways to build a hardware profile:

- Select a reference server and select **Clone Reference Server Settings** to extract all BIOS, BOOT, RAID, and iDRAC configuration settings on that server at that instant and apply them to the target system. These settings cannot be customized by the user.
- Select a reference server and select **Customize Settings from Reference Server** to extract all BIOS, BOOT, RAID, and iDRAC configuration settings on that server at that instant, and then customize them as needed before they are applied to a target system.

  **NOTE:** Setting the RAID configuration to **Customize** mode creates a RAID1 array and a dedicated hot-spare when possible.

To create a new hardware profile:

1. From the management center, select **Deployment - Deployment Templates - Hardware Profile**.
2. Click **Create New**. The **Hardware Profile**: **Profile Name** pop-up displays.
3. Enter the **Profile Name** and an optional **Description** that can be used to help manage custom hardware configurations.
4. Click **Save**. To continue, click **Reference Server** in the left pane. The Reference Server window is displayed.

5 Click **Edit**, and the Reference Server window becomes active. Click **Browse.**

6 A **Servers** pop-up displays; use the pop-up to highlight a server and click **Select**. To clone the reference server, continue to the next step. To customize the reference server settings, go to step 8.

7 To extract all hardware settings from the reference server, select the **Clone Reference Server Settings** radio button; no settings may be customized. Click **Save.** A pop-up that states extracting the settings will take several minutes is displayed; click **Continue.** The settings are populated, and the selected server's name, iDRAC IP address, and service tag are displayed in the **Reference Server** window. Go to step 15.

8 To provide the reference server hardware settings as defaults that can be customized, select the **Customize Settings from Reference Server** radio button. Click **Save.** A pop-up that states extracting the settings will take several minutes is displayed; click **Continue.** The settings are populated, and the selected server's name, iDRAC IP address, and service tag are displayed in the **Reference Server** window.

9 Select **Boot Order** from the left pane. To include boot order information in the profile, select the **Include Boot Order in this Hardware Profile** check box. Expand **Boot Order** to display the boot order options, and click **Edit** to make updates:

   a Use the **Boot Mode** drop-down menu to select either **BIOS** or **UEFI.**

   b Use the **View/Configure** drop-down menu under **Boot Device Sequence** to display the available boot devices. To make changes to the boot device sequence displayed, select the device and click either **Move Up** or **Move Down**.

   c Select **Enabled** in the **Boot Retry Sequence** drop-down menu so that the server automatically retries the boot sequence, or select **Disabled** to not retry the sequence.

   d Click **Save** to save the changes, or **Cancel** to cancel the changes.

10 If the **BIOS** boot mode was selected in step 9, you can expand **Hard Drive Sequence** to display the hard drive sequence options, and click **Edit** to make updates:

   a To make changes to the hard drive sequence displayed, select the device and click either **Move Up** or **Move Down**.

b Click **Save** to save the changes, or **Cancel** to cancel the changes.

**11** Select **BIOS Settings** from the left pane. To include BIOS setting information in the profile, select the **Include BIOS Settings in this Hardware Profile** check box. Expand a category to display the setting options, and click **Edit** to make updates to one of the following:

- Memory Settings
- Processor Settings
- SATA Settings
- Integrated Devices
- Serial Communication
- Embedded Server Management
- Power Management
- System Security
- Miscellaneous Settings

Once all updates are made for a category, click **Apply** to save the changes or click **Cancel** to cancel the changes.

**NOTE:** For detailed BIOS information, including setting options and explanations, refer to the *Hardware Owner's Manual* for the selected server.

**12** Select **iDRAC Settings** from the left pane, and select **Network**. To include network setting information in the profile, select the **Include Network Settings in this Hardware Profile** check box. Expand a category to display the setting options, and click **Edit** to make updates to one of the following:

- Network
- Network Settings
- Virtual Media

Once all updates are made for a category, click **Apply** to save the changes or click **Cancel** to cancel the changes.

**NOTE:** For detailed iDRAC information, including setting options and explanations, refer to the *iDRAC User's Guide* for the selected server.

13 Select **iDRAC Settings** from the left pane, and select **User List**. To include user list information in the profile, select the **Include User List in this Hardware Profile** check box. Under **iDRAC Local User List**, select a task to do the following:

- **Add User -** Manually enter an iDRAC user and the required information. When finished, click **Save** to save your changes or **Cancel** to cancel.
- **Delete User** - Delete the selected user. Select the check box for the user and click **Delete**, or click **Cancel** to cancel.
- **Edit User** - Manually edit an iDRAC user's information. When finished, click **Save** to save your changes or **Cancel** to cancel.

**NOTE:** For detailed iDRAC information, including setting options and explanations, refer to the *iDRAC User's Guide* for the selected server.

14 Select **RAID Configuration** from the left pane. To include RAID configuration information in the profile, select the **Include RAID Configuration in this Hardware Profile** check box. The window is updated with all RAID information.

15 The profile is saved, and displays in the **Hardware Profiles** window under **Available Profiles.**

## Managing Hardware Profiles

There are several management actions an administrator can perform on existing hardware profiles, including viewing/editing, duplicating, renaming, deleting, and refreshing.

To view/edit a hardware profile:

1 From the management center, select **Deployment - Deployment Templates - Hardware Profile**.

2 Select a profile and click **View/Edit**. The **Hardware Profile: Profile Name** window displays.

3 Select the profile section to display or change, and make any necessary changes.

4 Click **Save** to apply changes, or click **Cancel** to cancel changes.

To duplicate a hardware profile:

1. From the management center, select **Deployment - Deployment Templates - Hardware Profile**.
2. Select a profile and click **Duplicate**. The **Duplicate** pop-up displays.
3. Enter a unique hardware profile name.
4. Click **Apply** to create a copy of the profile with the new name, or click **Cancel** to cancel.

To rename a hardware profile:

1. From the management center, select **Deployment - Deployment Templates - Hardware Profile**.
2. Select a profile and click **Rename**. The **Rename Profile** pop-up displays.
3. Enter a unique hardware profile name.
4. Click **Apply** to use the new name, or click **Cancel** to cancel.

To delete a hardware profile:

1. From the management center, select **Deployment - Deployment Templates - Hardware Profile**.
2. Select a profile and click **Delete**; a message is displayed.
3. Click **Delete** on the message box to remove the profile, or click **Cancel** to cancel.

   **NOTE:** Deleting a hardware profile that is part of a running deployment task can cause the task to fail.

To display updated hardware profile information, from the management center, select **Deployment - Deployment Templates - Hardware Profile** and click **Refresh**.

## Configure a Hypervisor Profile

To deploy and configure ESX/ESXi software to a server, a hypervisor profile must be created. A hardware profile requires the following information:

- The scriptable Reference ISO software media location on an NFS share
- vCenter instance that manages the deployed hosts, plus an optional host profile
- The destination cluster or datacenter where the plug-in deploys servers in vCenter

**NOTE:** The following naming convention must be used for the Reference ISO file name:

```
host:/share/hypervisor.iso
```

```
\\host\share\hypervisor.iso
```

### Create New Hypervisor Profile

To create a new hypervisor profile:

1. From the management center, select **Deployment - Deployment Templates - Hypervisor Profile**.
2. Click **Create New** and the **Hypervisor Profile**: **Profile Name** pop-up displays.
3. Enter the **Profile Name** and an optional **Description** that can be used to help manage custom hypervisor profiles, and click **Save**.
4. Click **Reference ISO** in the left pane click **Edit,** and enter the following information:
   a. **Hypervisor Reference ISO**: A hypervisor ISO image (ESX 4.1, ESXi 4.1 and ESXi 5.0 only) on a share location; a copy of this hypervisor image will be modified to permit a scripted installation. The reference ISO location must be in the following format:
      - `host:/share/hypervisor.iso`
      - `\\host\share\hypervisor.iso`
   b. If using a CIFS share, enter the **User Name, Password,** and **Verify Password;** the passwords must match.
5. Click **Save** to add the settings to the profile.
6. Click **vCenter Settings** in the left pane click **Edit** and enter:
   - **vCenter instance**: Instance that will manage a host after deployment
   - **vCenter Destination Container**: Datacenter or cluster that hosts the new physical server(s); click **Browse** to search for vCenter destinations
   - **vCenter Host Profile**: A profile that encapsulates host configuration and helps to manage host configuration
7. Click **Save** to add the information to the profile.

### Managing Hypervisor Profiles

There are several management actions an administrator can perform on existing hypervisor profiles, including viewing/editing, duplicating, renaming, deleting, and refreshing.

To view or edit a hypervisor profile:

1. From the management center, select **Deployment - Deployment Templates - Hypervisor Profile**.
2. Select a profile and click **View/Edit**. The **Hypervisor Profile**: **Profile Name** window displays.
3. Select the profile section to display or change, and make any necessary changes.
4. Click **Save** to apply changes, or click **Cancel** to cancel changes.

To duplicate a hypervisor profile:

1. From the management center, select **Deployment - Deployment Templates - Hypervisor Profile**.
2. Select a profile and click **Duplicate**. The **Duplicate** pop-up displays.
3. Enter a unique hypervisor profile name.
4. Click **Apply** to create a copy of the profile with the new name, or click **Cancel** to cancel.

To rename a hypervisor profile:

1. From the management center, select **Deployment - Deployment Templates - Hypervisor Profile**.
2. Select a profile and click **Rename**. The **Rename Profile** pop-up displays.
3. Enter a unique hypervisor profile name.
4. Click **Apply** to use the new name, or click **Cancel** to cancel.

To delete a hypervisor profile:

1. From the management center, select **Deployment - Deployment Templates - Hypervisor Profile**.
2. Select a profile and click **Delete**; a message is displayed.
3. Click **Delete** on the message box to remove the profile, or click **Cancel** to cancel.

**CAUTION: Deleting a hypervisor profile that is associated with scheduled deployment jobs can cause the deployment jobs to fail.**

To display updated hypervisor profile information, from the management center select **Deployment - Deployment Templates - Hypervisor Profile** and click **Refresh**.

# Building a Deployment Template

A deployment template contains either a hardware profile, a hypervisor profile, or both. The **Deployment Wizard** uses this template to provision server hardware and deploy hosts within vCenter. To create a new deployment template:

1. From the management center, select **Deployment - Deployment Templates.**
2. Click **Create New.** The **Create New** window displays; enter a name for the template and click **Save**.
3. Click **Edit** to complete the template. The right pane displays the **Hardware Profile** and **Hypervisor Profile** drop-down menus.
4. From the **Profile** drop-down menu, choose a profile. There are several actions that can be performed on the selected profile:
   a. Click **View** to display the hardware/hypervisor profile settings for the selected profile.
   b. Click **Create New** to create a new hardware/hypervisor profile.
5. Enter an optional **Description** for the deployment template that can be used to help manage the templates.
6. Click **Save** to apply profile selections and save changes, or click **Cancel** to cancel.

## Managing Deployment Templates

There are several management actions an administrator can perform on existing deployment templates, including duplicating, renaming, deleting, and refreshing.

To duplicate a deployment template:

1. From the management center, select **Deployment - Deployment Templates.**

2. Select a template and click **Duplicate**.
3. Enter the template's new name and click **Apply**. If a template already exists with that name, the apply action will not be successful.

To delete a deployment template:

1. From the management center, select **Deployment - Deployment Templates.**
2. Select a template and click **Delete**.
3. Click **Delete** on the message box to delete the template, or click **Cancel** to cancel.

   **NOTE:** Deleting a hardware profile that is part of a running deployment task can cause the task to fail.

To rename a deployment template:

1. From the management center, select **Deployment - Deployment Templates.**
2. Select a template click **Rename** to display the **Rename Template** pop-up.
3. Enter the template's new name and click **Apply**. If a template already exists with that name, the apply action will not be successful.

To display all updated deployment templates, from the management center select **Deployment - Deployment Templates** and click **Refresh**.

# Running the Deployment Wizard

The **Deployment Wizard** steps you through the bare-metal server deployment process of:

- Selecting undeployed servers
- Using a deployment template (hardware and hypervisor profiles combination)
- Assigning identification to the deployed servers
- Matching a desired connection profile to each server
- Scheduling the server deployment jobs to run
- Displaying the **Job Queue** where you can manage deployment jobs.

  **NOTE:** Deployment of ESXi to internal Secure Digital (SD) cards is not supported.

Use the **Next** and **Back** controls to navigate through the wizard panels.

The Deployment Wizard steps you through each phase of the deployment process:

1. From the management center, select **Deployment - Deployment Wizard**. The **Select Servers** window is displayed**.**
2. **Select Servers** assigns non-deployed servers to this deployment job. Select the servers using the check boxes and click **Next**.
3. **Deployment Template** selects/creates a deployment template in one of several ways:
   - Select an existing deployment template under **Available Templates**. Information for the selected template populates the right pane.
   - Select an existing deployment template and click **Edit** to change one or both associated profiles.
   - Click **Create New** to define a new template.

   Once the deployment template is selected/created, click **Next.**
4. **Server Identification** assigns deployed servers new names and network identification.
   a. Click **Non-Compliant Servers** to display a list of servers that do not meet the minimum requirements for firmware, BIOS, or have other issues; click **Details** for additional information. Once the systems are updated, click **Check Compliance** to retest and verify fixes. Click **Refresh** to refresh the list, and click **Abort All Test** to cancel the testing.
   b. Click ^ to expand and view individual server information.
   c. Under **Host Name and NIC**, enter a **Fully Qualified Host Name** for the server. In the **NIC Management Tasks** drop-down menu, select the NIC that will be used for managing the server.
   d. Enter IP addresses, subnet mask and other network information, or select the **Obtain using DHCP** check box.
   e. Repeat for all servers to deploy, or select the **Apply settings to all selected servers** check box.

   Once server identification information is entered, click **Next.**

5 **Connection Profile** automatically assigns servers to connection profiles after the deployment job completes.

   a Select the **Assign all servers to the same connection profile** radio button, and select the connection profile from the drop-down menu to assign all servers to the same existing profile. To create a new profile, click **New** and to view or edit the select profile click **View/Edit**.

   a Click **View** to display the selected connection profile settings.

   b Select the **Select a Connection Profile for each Server** radio button, and select an individual connection profile for each server from the drop-down menu.

   Once a connection profile is selected, click **Next.**

6 **Schedule** sets the schedule for the deployment job. There are several options of when to run the deployment job: immediately, schedule the deployment job to run on a selected date and time, hold deployment job and manually start it.

   a Determine when to run a deployment job by entering a date and time:

   - Click **Schedule server(s) for deployment**.
   - Use the calendar control to select the date.
   - Enter the time of day:

   Immediately: Click **Deploy server(s) now**.

   Postpone job: Click **Create deployment job, but put on hold**; with this option, only the schedule can be modified and all other deployment job options cannot be changed.

   b Enter a **Job Name** and **Job Description**.

   c Click **Finish**.

7 Now that the deployment wizard is complete, you can manage deployment jobs using the Job Queue.

8 Click **Non-Compliant Servers** to display a list of non-compliant servers that must have a firmware update before the wizard can be completed.

## Managing Deployment Jobs Using the Deployment Job Queue

To mange deployment jobs using the **Job Queue:**

1. From the management center, select **Job Queue- Deployment Jobs.**
2. To update **Deployment Jobs Details** click **Refresh**. Updated deployment job information—status, scheduled time, name, description, collection size, and progress summary—is displayed.
3. Click **Details** to display a **Deployment Job Details** pop-up window that contains detailed information on the servers included in the deployment job such as:
   - Service tag
   - iDRAC IP address
   - Server status
   - If any warnings occurred
   - Deployment job details
   - Start and End time

   To display full information for each item in the pop-up's table, hover over the item and an additional text pop-up is displayed.
4. Click **Modify** to display a pop-up to either put a selected job on hold or to enter an updated schedule.
5. Click **Abort** to abort the deployment job; click **Abort Job** on the displayed message to abort, or click **Do Not Abort Job** to cancel.

   **NOTE:** Any deployment jobs that are in progress cannot be aborted.
6. Click **Purge Job Queue** to display the **Purge Deployment Job Queue** window. Select the **Older than:** date and job **Status**, and click **Apply.** The select jobs are then cleared from the queue.

# Server Security Settings for Deployment

The set of deployable servers can be restricted using a *white list*. If a server is in the white list, it is provided with credentials during the auto-discovery and handshake process and shows up in the list of servers that can be used for deployment. The white list can be maintained by manually adding server service tags, deleting service tags, or importing a list of service tags from a CSV file.

**NOTE:** A CSV-delimited file can be used to import servers, and can contain multiple records on different lines where each record has one or more service tags separated by commas.

To enable a server white list:

1. Select **Security** under **Settings**, and click **Edit**.
2. Select the **Enforce Server White List** check box to use the white list to restrict server deployment.
3. Click **Apply**, and **The server white list is:** setting changes to **ENABLED**.

To add servers to the white list:

1. Click **Edit**, and then click **Add Server**.
2. When the **Enter service tags to add to the white list** pop-up displays, enter the service tags.
3. Click **Continue** to add the tags.
4. To import a list of service tags, click **Import White List**.
5. When the **Select File to Upload (client IP address)** displays, navigate to the CSV file and click **Open**.
6. When the **We found these service tags in your file** pop-up displays, click **Apply**.

To delete servers from the white list:

1. To delete an individual server, click the service tag check box and click **Delete Selected**.
2. To delete all servers, click the **Service Tag** check box and then click **Delete Selected.**
3. Click **Apply** when the **Are you sure you want to delete the selected service tags** pop-up displays to finish the delete, or click **Cancel** to cancel.
4. Click **Apply** to complete the changes to the white list.

# 5

# Firmware Updates

The location where servers receive firmware updates is a global setting that is available in the management center. It can also be a local setting, used only on an individual server. By having the ability to determine the firmware update location, different updates can be applied to different sets of servers.

## Enter Global Firmware Repository Location

Firmware repository settings contain the firmware catalog location used to update deployed servers. There are two location types:

- Dell online (ftp.dell.com) - Uses the default firmware update repository of Dell online (ftp.dell.com) with a required staging folder. The Plug-in will download selected firmware updates and store them in the staging folder, and then they are applied as necessary.
- Local/shared repository - Created with the Dell Repository Manager™ application. These local repositories should be located on Windows-based file shares.

  **NOTE:** Using the latest version of Dell Repository Manager to create an update repository is recommended. Once the repository is created, save it to a location that the registered hosts can access. Repository passwords cannot exceed 31 characters.

To enter the repository location and credentials:

1. From the management center, select **Settings - Firmware Repository** and click **Edit**.
2. Select the **Dell online (ftp.dell.com)** radio button to use the Dell online repository location. Perform the following steps:
   a. Enter the **Staging Folder Location** using the following format:

      *host:/share* or *\\host\share*

      **NOTE:** When using a firmware repository on a network share, it must reside on a CIFS or NFS share that is accessible to the virtual appliance. Credentials are required for accessing CIFS share (add domain to user name field if required.) The user must have read and write access on the share.

b If using a CIFS share for the staging folder, enter the **User Name, Password,** and **Verify Password**; the passwords must match. These fields are only active when entering a CIFS share.

c Click **Begin Test** to validate your entries.

3 Select **Shared Network Folder** radio button to use a local/shared repository location. Perform the following steps:

a Enter the **Catalog File Location** using the following format:

```
host:/share/filename.xml,
host:/share/filename.gz,
\\host\share\filename.xml,
\\host\share\filename.gz
```

b If using a CIFS share, enter the **User Name, Password,** and **Verify Password**; the passwords must match. These fields are only active when entering a CIFS share.

**NOTE:** The @ character is not supported for use in shared network folder user names/passwords.

c Click **Begin Test** to validate your entries.

4 Click **Apply**. The repository update location is now saved.

# Update Individual Server Firmware

To perform a firmware update for the host system:

1 From the **Dell** tab, select **Run Firmware Update Wizard** to launch the window.

2 For **Select an Update Source**, select the update source:

- **Load a single firmware update from a file** - Enter the UNC path to a Dell Update File (DUP) that is an executable file (.EXE); the path must be accessible to the Management Plug-In virtual appliance and iDRAC. Enter the required user name and password to access the file, and click **Next**. Skip to step 5.
- **Update from a repository** - Use the default firmware update repository of Dell Online (ftp.dell.com) that is used with a required staging folder. The Plug-in will download selected firmware updates from Dell Online and store them in the staging folder, and then they are applied

as necessary. A local repository created with Dell Repository Manager that is accessible on a network shared folder may also be used. Click the radio button and click **Next**. Continue to step 3.

**NOTE:** If the required staging folder is not configured, an error is generated.

3. Select the update bundle from the drop-down menu, and click **Next**.
4. Select the updates to apply from the bundle, and click **Next**. Updates with the same version are disabled, and updates with a lower version will attempt a downgrade action.
5. Select the server restart method and click **Finish**:
   - **Enter maintenance mode, apply update(s), and reboot** - The host is put into maintenance mode before applying the update. If the host cannot enter maintenance mode, then it will automatically reboot and the update is applied after the reboot completes.
   - **Apply Update(s) after next reboot** - The update is applied after the next full reboot. To avoid service interruptions, it is recommended that the host is first put into maintenance mode before a reboot is attempted. Until the updates are applied, no further update job will be accepted by the host system's iDRAC.
   - **Apply update(s) and force reboot without entering maintenance mode** - The update is applied and a reboot occurs even if the host system is not in maintenance mode. This option is not recommended.
6. To verify that the update was successful, rerun the **Inventory Job** using **Job Queue – Run Now**, and review the **Overview** page to see the new versions.

# 6

# Management Plug-In Administration

Administration of the Management Plug-in and its virtual environment is achieved by using two additional administration portals: a Web-based administration portal and the Console view for an individual server. Through the use of these two portals, global settings for vCenter management, plug-in database backup and restore, and reset/restart actions can be entered and used across all vCenter instances.

## Web-based Administration Portal

The Web-based administration portal provides several key pieces of functionality: vCenter server registration and management, virtual appliance management, global vCenter alert settings, and backup and restore settings.

### vCenter Registration

The **vCenter Registration** window allows you to register a vCenter server, and to upload a license. When a new Management Plug-In is installed, it must be registered with the vCenter server on which it is installed. To register a new vCenter server:

1. Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:
   **https://<ApplianceIPAddress>/DellAdminPortal/index.html**
2. Click **VCENTER REGISTRATION** in the left pane. Click **Register New vCenter Server** to register a new server.
3. Enter the user name, password, and vCenter IP address. Click **Apply** to register the Plug-in, or click **Cancel** to cancel.

To modify the administrator login for the registered vCenters:

1. Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

**https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2. Click **VCENTER REGISTRATION** in the left pane. The registered vCenters are displayed in a table. Click **Modify** under **Credentials** to display the **Modify Admin Acct** window.
3. Enter the **User Name, Password,** and **Verify Password**; the passwords must match. Click **Apply** to change the password, or **Cancel** to cancel the change.

To update the SSL certificates for the registered vCenters:

1. Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

   **https://<ApplianceIPAddress>/DellAdminPortal/index.html**
2. Click **VCENTER REGISTRATION** in the left pane. The registered vCenters are displayed in a table. Click **Update** to update the certificates.
3. When a new client accesses

To unregister a vCenter:

1. Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

   **https://<ApplianceIPAddress>/DellAdminPortal/index.html**
2. Click **VCENTER REGISTRATION** in the left pane. The registered vCenters are displayed in a table. Click **Unregister** to display the unregister pop-up; click **Unregister** to complete the process.

When a new Management Plug-In is installed, the license file included in the download package must be uploaded using the administration portal. To upload the license file:

1. Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

   **https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2 Click **VCENTER REGISTRATION** in the left pane. The registered vCenters are displayed in a table. Click **Upload License** to display the upload license pop-up; click the **Browse** button to navigate to the license file. Click **Upload** to upload the license file.

**NOTE:** If the license file is modified, or edited in any way, the appliance will view it as corrupted and the file will not work.

## Virtual Appliance Management

Virtual appliance management contains the Management Plug-in network, version, NTP, and HTTPS information, and allows an administrator to:

- Restart the virtual appliance
- Update the virtual appliance, and configure an update repository location
- Generate a troubleshooting bundle that contains appliance logging information.
- Enter Network Time Protocol (NTP) settings
- Upload and manage HTTPS certificates

To restart the virtual appliance:

**NOTE:** Restarting the appliance will log out the user from the Administration Portal and the Plug-In will be unavailable until the appliance and its services are active.

1 Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

**https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2 Click **APPLIANCE MANAGEMENT** in the left pane. Click **Restart the Virtual Appliance** to restart the Management Plug-In virtual appliance.

3 On the **Restart Virtual Appliance** pop-up, click **Apply** to restart the appliance or click **Cancel** to cancel.

To configure an update repository location, and update the virtual appliance:

**NOTE:** Perform a backup prior to an update of the virtual appliance to make sure all data is protected.

1 Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

**https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2 Click **APPLIANCE MANAGEMENT** in the left pane. Click **Edit** next to **Appliance Update**. Enter the update repository host name or IP address into the active field. Click **Apply.** Once the update location is saved, click **Cancel** to exit.

**NOTE:** If the update location is on an external network, such as the Dell FTP site, then a proxy must be entered for the Plug-In using the Settings -> Proxy page in the main console.

3 Click **Update Virtual Appliance** to update the appliance to the software version listed under **Available Version**. An **Update Appliance** pop-up displays, listing the current and available versions. An appliance backup must be performed prior to an update, and all other management center and administration portal sessions must be closed. Click **Upgrade** to begin the update.

4 The system is locked down and put into maintenance mode. When the update is complete, the appliance page displays showing the new version installed.

To generate a troubleshooting bundle that contains virtual appliance logging information:

1 Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

**https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2 Click **APPLIANCE MANAGEMENT** in the left pane. Click **Generate Troubleshooting Bundle** to display the troubleshooting bundle pop-up.

3 Click the **Download Troubleshooting Bundle** link to either open or save a zip file that contains appliance logging information. This information can be used to assist in troubleshooting issues, or sent to Technical Support.

4 Click **Close** once the bundle is saved to exit.

Network Time Protocol (NTP) can be used to synchronize the virtual appliance and host systems clocks to that of a NTP server. To enter NTP server information:

1. Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

   **https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2. Click **APPLIANCE MANAGEMENT** in the left pane. Click **Edit** for **NTP**.
3. Select the **Enabled** check box to enable NTP. Enter the host name or IP address for a **Preferred** and **Secondary NTP Server** and click **Apply.**
4. Once the NTP server locations are saved, click **Cancel** to exit.

HTTPS Certificates can be used for secure communication between the virtual appliance and the host systems. To set-up this type of secure communication, a certificate signing request must be sent to a certificate authority and then the resulting certificate is uploaded using the Administration Portal. There is also a default certificate that is self-signed and can be used for secure communication; this certificate is unique to every installation.

To upload a certificate:

1. Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

   **https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2. Click **APPLIANCE MANAGEMENT** in the left pane. Click **Upload Certificate** for **HTTPS Certificates.** An upload certificates pop-up is displayed; click **OK.**
3. Click **Browse** to select the certificate to upload, and click **Upload.** The certificate must use PEM format. Click **Cancel** to cancel the upload.

To restore the default (self-signed) certificate:

1. Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

   **https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2 Click **APPLIANCE MANAGEMENT** in the left pane. Click **Restore Default Certificate** for **HTTPS Certificates.** A restore default certificate pop-up is displayed; click **Apply.**

To generate a signing request:

1 Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

**https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2 Click **APPLIANCE MANAGEMENT** in the left pane. Click **Generate Certificate Signing Request** for **HTTPS Certificates.** A pop-up displays stating that if a new request is generated certificates created using the previous CSR can no longer be upload to the appliance. Click **Continue** to continue with the request, or **Cancel** to cancel.

3 Enter the **Common Name, Organizational Name, Organizational Unit, Locality, State Name, Country** and **Email** for the request. Click **Continue** and the request is completed. Use the download link to download the new CSR for use.

### Global vCenter Alert Settings

Alert management allows an administrator to enter global settings for how alerts are stored for all vCenter instances. To enter global vCenter alert settings:

1 Launch a browser window, and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

**https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2 Click **ALERT MANAGEMENT** in the left pane; the current vCenter alert settings are displayed. Click **Edit** to enter new settings.

3 Enter numeric values for the following items:

- Maximum number of alerts
- Number of days to retain alerts
- Timeout for duplicate alerts (seconds)

4 Click **Apply** to save your changes, or click **Cancel** to cancel.

### Plug-in Database Backup and Restore

The backup and restore function backs up the plug-in database to a remote share from which it can be restored at a later date. Profiles, templates, and host information are included in the backup. It is recommended that you schedule automatic backups to guard against data loss.

To configure backup and restore:

1. Launch a browser window, and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

   **https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2. Click **BACKUP AND RESTORE** in the left pane, and the current backup and restore settings are displayed. Click the top **Edit** button to enter new backup location settings.
3. Enter the **Share, User Name, Password, Encryption Password,** and **Verify Password** for the backup location. Click **Apply** to save your changes or **Cancel** to cancel.
4. Click the bottom **Edit** button to enter a backup schedule. Click the **Enabled** radio button for **Schedule backups are currently** to enable the backups.
5. Select the days of the week check boxes for **Backups will occur on these days** to select the backup days.
6. Enter a 24-hour local time (hh:mm) for **At this time**, and click **Apply** to save your changes or **Cancel** to cancel.

To perform an immediate backup:

1. Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

   **https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2. Click **BACKUP AND RESTORE** in the left pane and the current backup and restore settings are displayed. Click **Backup Now** and a backup pop-up is displayed.
3. Enter a **Folder Path (CIFS/NFS Format), User Name, Domain, Password,** and **Encryption Password** for the backup.

4 Click **Apply** to save your changes and perform the backup, or click **Cancel** to cancel.

To schedule automatic backups:

1 Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

**https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2 Click **BACKUP AND RESTORE** in the left pane and the current backup and restore settings are displayed. Click **Edit** for **Automatic Scheduled Backup** to make the fields active.

3 Select the **Enabled** radio button to enable the backups. Select the check box for the days of the week and enter the time in 24 hour format (hh:mm). Click **Apply.**

4 The **Next Backup** will populate with the date and time of the next scheduled backup.

To restore the database from a backup:

1 Launch a browser window and enter the **Administration Portal URL** displayed in the **Console** tab. The URL uses the following format and is case sensitive:

**https://<ApplianceIPAddress>/DellAdminPortal/index.html**

2 Click **BACKUP AND RESTORE** in the left pane and the current backup and restore settings are displayed. Click **Restore Now** and a restore pop-up is displayed.

3 Enter a **Backup File Path (CIFS/NFS Format)**, or use the **Browse** button to navigate to a folder location.

4 Enter the **User Name, Password,** and **Encryption Password** for the backup.

5 Click **Apply** to save your changes and perform the restore operation, or click **Cancel** to cancel. The restore operation will cause the virtual appliance to reboot after it is complete.

# Console View

The console view provides the ability to configure network settings, change the administration password, set the local time zone, reboot the virtual appliance, reset the virtual appliance to the factory settings, and refresh the virtual appliance console view.

### Configure Network Settings

To configure network settings:

1. Select the plug-in virtual machine, click the **Console** tab, select **Configure Network,** then press **<Enter>.**
2. Enter the desired network settings under **Edit Devices** or under **Edit DNS configuration,** then click **Save & Quit.** To not make any changes, click **Quit.**

### Change Virtual Appliance Administration Password

To change the virtual appliance administration password:

1. Select the plug-in virtual machine and click the **Console** tab, then select **Change Admin Password** and press **<Enter>.**
2. Enter the **Current Admin Password** and press **<Enter>.**
3. Enter a new password for **Enter new Admin Password** and press **<Enter>.**
4. Enter the new password again for **Please Confirm Admin Password** and press **<Enter>**. The administration password is changed.

### Set Local Time Zone

To set the virtual appliance local time zone:

1. Select the plug-in virtual machine and click the **Console** tab, then select **Set Time Zone** and press **<Enter>.**
2. Use the **Timezone Selection** window to select the desired time zone and click **OK.** To cancel changes click **Cancel.** The time zone is updated.

### Reboot Virtual Appliance

To reboot the virtual appliance:

1. Select the plug-in virtual machine and click the **Console** tab, then select **Reboot this Virtual Appliance** and press **<Enter>**.
2. The following message is displayed:

   ```
   If there are any processes running on this
   appliance they will be terminated by this action.
   Are you sure you wish to do this?
   ```

   Enter **y** to reboot or **n** to cancel. The appliance is rebooted.

### Reset Virtual Appliance to Factory Settings

To reset the virtual appliance to the factory settings:

1. Select the plug-in virtual machine and click the **Console** tab, then select **Reset this Virtual Appliance to Factory Settings** and press **<Enter>**.
2. The following notice is displayed:

   ```
   This operation is completely Irreversible if you
   continue you will completely reset *this*
   appliance to its original settings. All changes
   you have made to this appliance will be Lost. Are
   you sure you wish to Reset this Appliance to
   Factory Settings?
   ```

   Enter **y** to reset or **n** to cancel. The appliance is reset to the original factory settings.

   **NOTE:** When the virtual appliance is reset to factory settings, any updates made to the Network Configuration are preserved; these settings are not reset.

### Refresh Console Tab View

To refresh the Console view, select **Refresh** and press **<Enter>**.

### ReadOnly User Role

There is an unprivileged user role called **readonly** with shell access for diagnostic purposes. The **readonly** user has limited privileges to run the `mount`. The **readonly** user's password is set to the same as the **admin**.

# 7

# Troubleshooting

## Upgrade

**I backed up my 1.0 appliance, powered it off, deployed 1.0.1 and tried to restore my database. The Plug-in is disabled. What do I do?**

The 1.0 appliance must be unregistered before it is powered off. Follow the supported upgrade procedure in this book for more details.

**I backed up my 1.0 appliance, unregistered it, deployed 1.0.1 and registered it, and then restored the database. An unknown error was displayed when I tried to start the Plug-in Management Console in vSphere. What do I do?**

Power off the 1.0.1 appliance and power on the 1.0 appliance. Follow the supported upgrade procedure in this book for more details.

**I unregistered my 1.0 appliance, backed up the database, deployed 1.0.1 and registered it, and then restored the database. When I start the Plug-in Management Console, I get a message that states the vCenter is not registered. The Administration Portal has no registered vCenters displayed, and when I try to register one I get an error message that says it is registered already. What do I do?**

You must manually unregister the extension by accessing the vCenter Managed Object browser. Then you must re-register the vCenter with the Plug-in using the Administration Portal.

## Common Questions

**How do I test event settings by using OMSA to simulate a temperature hardware fault?**

To make sure that events are functioning correctly:

1. Navigate to **Alert Management –> Platform Events** in the OMSA user interface.
2. Select the **Enable Platform Event Filter Alerts** check box.

3 Scroll down to the bottom, and click **Apply Changes**.

4 To make sure that a specific event is enabled, such as temperature warning, select **Main System Chassis** from the tree view on the left.

5 Select **Temperatures** under **Main System Chassis**.

6 Select the **Alert Management** tab, and select **Temperature Probe Warning**.

7 Select the **Broadcast a Message** check box, and select **Apply Changes**.

8 To cause the temperature warning event, select **Main System Chassis** from the tree view on the left.

9 Select **Temperatures** under **Main System Chassis**.

10 Select the **System Board Ambient Temp** link, and select the **Set to Values** radio button.

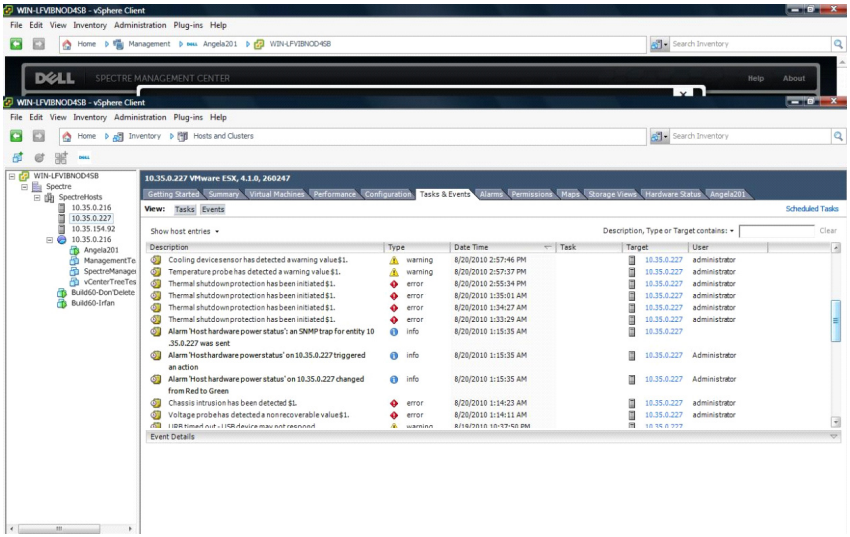
11 Set the **Maximum Warning Threshold** to *below* the current listed reading; for example if the current reading is 27, set the threshold to 25.

12 Select **Apply Changes**, and the temperature warning event is generated. To cause another event, restore the original settings using the same **Set to Values** option. Events are generated as warnings, and then to a normal state.

If everything is working properly, navigate to the vCenter **Tasks & Events** tab, and select the **Events** view; a temperature probe warning event should be displayed.

**NOTE:** There is a filter for duplicate events; if you try to trigger the same event too many times in a row, you will only receive one event. Allow at least 30 seconds between events to see all events.

**Figure 7-1. Simulated temperature event**


WIN-LFVIBNOD45B - vSphere Client
File Edit View Inventory Administration Plug-ins Help
SPECTRE MANAGEMENT CENTER
Help About
10.35.0.227 VMware ESX, 4.1.0, 260247
Getting Started Summary Virtual Machines Performance Configuration Tasks & Events Alarms Permissions Maps Storage Views Hardware Status Angela201
Description Type Date Time Task Target User
Event Details

### I have the OMSA agent installed on a Dell host system, but I still get an error message that OMSA is not installed. What should I do?

To resolve this issue, install OMSA with the *Remote Enablement* component on the host system. If you are using the command line to install OMSA, make sure to specify the `-c` option. If OMSA is already installed, reinstall it with the `-c` option and restart the service:

```
srvadmin-install.sh -c

srvadmin-services.sh restart
```

For an ESXi host, you must install OMSA VIB using the VMware Remote CLI tool, and reboot the system.

### Why do I see auto-discovered systems without model information in the deployment wizard?

This usually indicates that the firmware version installed on the system does not meet recommended minimums.

In some cases, a firmware update may not have registered on the system; cold booting the system or reseating the blade fixes this problem. The newly-enabled account on the iDRAC must be disabled and auto-discovery re-initiated to provide model info and NIC information to the plug-in.

#### Can the plug-in support ESX/ESXi with Lockdown mode enabled?

No. Lockdown mode is not supported in this release.

#### What setting should I use for UserVars.CIMoenProviderEnabled with ESXi 4.1 U1?

UserVars.CIMoemProviderEnabled must be set to 1.

#### Can the plug-in support multiple vCenters in linked mode?

No. The Plug-in does not support multiple vCenters in linked mode.

#### I am using a reference server to create a Hardware Profile, but it failed. What should I do?

Check to make sure that minimum recommended versions of iDRAC firmware, Lifecycle Controller firmware, and BIOS are installed.

To make sure that the data retrieved from the reference server is current, enable Collect System Inventory On Restart (CSIOR), and restart the reference server prior to extraction of data. See "Setting Collect System Inventory on Restart (CSIOR) on a Clone Server" on page 65 for more information.

#### I am attempting to deploy ESX/ESXi on a blade server, and the deployment job failed. What should I do?

1. Make sure the ISO location (NFS path) and staging folder paths are accurate.
2. Make sure the NIC selected during assignment of server identity is on the same network as the Dell appliance.
3. If using static IP assignment, make sure the network information provided (including subnet mask and default gateway) is accurate. Also, make sure the IP address is not already assigned on the network.
4. Make sure at least one Virtual Disk is seen by the system; ESXi does not install to the internal SD module.

**The NFS share is set up with the ESX/ESXi ISO, but deployment fails with errors mounting the share location. What should I do?**

1. Check the NFS setup to make sure complete read/write access is configured for the staging folder.
2. If a staging folder is not used, make sure the location of the original ISO has full read/write access.
3. If the error message indicates that permissions were denied to the root user for mounting the NFS share, then the issue could stem from a known issue with installing ESX on a slow network. Append additional sub-directories for the staging folder.

**How do I force removal of the Dell appliance?**

If the Plug-in Admin Portal cannot be used to unregister the appliance, force removal as follows:

1. Go to https://<vcenter_server_IPaddress>/mob
2. Click **Content.**
3. Click **ExtensionManager**.
4. Click **UnregisterExtension.**
5. Enter the extension key to unregister **com.dell.plugin.Dell Management Plug-in**, then click **Invoke method.**
6. In the vSphere client, power off the plug-in appliance and delete it.

**I entered a password in the BACKUP NOW screen of the Administration Console and clicked Apply, but I am getting an error message that the Encryption Password is invalid. What should I do?**

If you are using the low resolution monitor, the **Encryption Password** field will not be visible from the **BACKUP NOW** screen. You must scroll down the page to enter the encryption password.

**I clicked the Dell Tab, or Dell Management Center icon from the vSphere client, and I get a 404 ERROR PAGE NOT FOUND error. What should I do?**

Check if the appliance is running; if not, then restart it from the vSphere client. Wait for a few minutes for the appliance Web service to start, and refresh the page. If the error continues, try and ping the appliance using the

IP address or fully-qualified domain name from a command line. If the ping does not resolve, review your network settings to make sure they are correct.

#### My firmware update failed, what do I do?

Check the appliance logs to see if the tasks timed out. If so, iDRAC needs to be reset by performing a cold reboot. Once the system is up and running, check to see if the update was successful by either running an inventory or using the **Firmware** tab.

#### My vCenter registration failed, what can I do?

vCenter registration can fail due to communication issues, therefore if you are experiencing these issues one solution is to use a static IP address. To use a static IP address, in the **Console** tab of the Plug-in virtual machine and select **Configure Network -> Edit Devices** and enter the correct gateway and FQDN (fully-qualified domain name). Enter the DNS server name under **Edit DNS Config**.

**NOTE:** Make sure that the appliance can resolve the DNS server you entered.

# Bare-Metal Deployment

## Auto-Discovery and Handshake Prerequisites

- Prior to running auto-discovery and handshake, make sure that iDRAC and Lifecycle Controller firmware and BIOS versions meet the minimum recommendations.
- CSIOR must have run at least once on the blade.

## Hardware Configuration Failure

- Before initiating a deployment task, ensure the system has completed CSIOR and is not in the process of rebooting.
- It is highly recommended that BIOS configuration be run in Clone mode, so that the reference server is an identical system.
- In Custom mode, the Plug-in does not manage dependencies between BIOS attributes.

- Some controllers do not allow creation of a RAID 0 array with one drive. This feature is supported only on high-end controllers, and the application of such a hardware profile can cause failures.

### Enabling Auto-Discovery on a Newly-Purchased System

The auto-discovery feature of a host system is not enabled by default; instead, enablement must be requested at the time of purchase.

If auto-discovery was not requested at the time of purchase, it can be enabled as follows:

1. During the boot process, press `ctrl-E`. The iDRAC setup screen displays.
2. Enable the NIC (blade servers only).
3. Enable auto-discovery.
4. Enable DHCP.
5. Disable admin accounts.
6. Enable **Get DNS server address from DHCP**.
7. Enable **Get DNS domain name from DHCP**.
8. In the **Provisioning Server** field, enter:

   ```
   <Dell Management Plug-in appliance IP
   address>:4433
   ```

If auto-discovery enablement is requested at the time of purchase, DHCP is enabled on the iDRAC and admin accounts are disabled. It is not necessary to configure a static IP address for the iDRAC; it will get one from a DHCP server on the network. To make use of the auto-discovery feature, a DHCP server or a DNS server (or both) must be configured to support the discovery process. CSIOR has already been run by factory process.

For more information on how to set up a network to support auto-discovery, see the *Dell Auto-Discovery Network Setup Specification* at **http://attachments.wetpaintserv.us/xBUlrs4t%2B2TzbrwqYkblvQ%3D%3D262254**

# Contacting Dell

**NOTE:** If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Visit **support.dell.com**.
2. Select your support category.
3. If you are not a U.S. customer, select your **country code** at the bottom of the page, or click **All** to see more choices.
4. Select the appropriate service or support link based on your need.

# Where to get additional help for this software

View or download Dell virtualization documentation:

**http://support.dell.com/support/edocs/software/eslvmwre/.**

Dell vCenter Plug-In Frequently Asked Questions
**http://i.dell.com/sites/content/business/solutions/virtualization/en/Documents/dell-management-plugin-vmware-vcenter-faq.pdf**

# Dell Management Plug-in for VMware vCenter Related information

- View or download VMware vSphere 4d for Dell PowerEdge Servers **http://support.dell.com/support/edocs/software/eslvmwre/VS/index.htm**.
- View or download Dell server documentation for PowerEdge™ Servers at: **http://support.dell.com/support/systemsinfo/documentation.aspx?c=us&l=en&s=gen&~subcat=88&~cat=12.**
- Dell OpenManage System Administrator documents **http://support.dell.com/support/systemsinfo/documentation.aspx?c=us&l=en&s=gen&~subcat=108&~cat=6.**
- Dell common glossary **http://support.dell.com/support/edocs/SOFTWARE/common/glossary.pdf**.

- Dell Lifecycle Controller documentation **http://support.dell.com/support/edocs/software/smusc/smlc/.**
- Dell Lifecycle Controller Overview **http://content.dell.com/us/en/enterprise/d/business~solutions~whitepapers~en/Documents~lifecycle-controller-dell.pdf.aspx.**

# A

# Virtualization-Related Events

The following table contains the virtualization-related critical and warning events, including event name, description and severity level.

| Event Name | Description | Severity | Recommended Action |
|---|---|---|---|
| Dell - Current sensor detected a warning value | A current sensor in the specified system exceeded its warning threshold. | Warning | No action |
| Dell - Current sensor detected a failure value | A current sensor in the specified system exceeded its failure threshold. | Error | Put the system into maintenance mode |
| Dell - Current sensor detected a non-recoverable value | A current sensor in the specified system detected an error from which it cannot recover | Error | No action |
| Dell - Redundancy regained | Sensor Returned to Normal Value | Info | No action |
| Dell - Redundancy degraded | A redundancy sensor in the specified system detected that one of the components of the redundancy unit has failed but the unit is still redundant. | Warning | No action |

| Event Name | Description | Severity | Recommended Action |
|---|---|---|---|
| Dell - Redundancy lost | A redundancy sensor in the specified system detected that one of the components in the redundant unit has been disconnected, has failed, or is not present. | Error | Put the system into maintenance mode |
| Dell - Power supply returned to normal | Sensor Returned to Normal Value | Info | No action |
| Dell - Power supply detected a warning | A power supply sensor reading in the specified system exceeded a user-definable warning threshold. | Warning | No action |
| Dell - Power supply detected a failure | A power supply has been disconnected or has failed. | Error | Put the system into maintenance mode |
| Dell - Power supply sensor detected anon-recoverable value | A power supply sensor in the specified system detected an error from which it cannot recover. | Error | No action |
| Dell - Memory Device Status warning | A memory device correction rate exceeded an acceptable value. | Warning | No action |
| Dell - Memory Device error | A memory device correction rate exceeded an acceptable value, a memory spare bank was activated, or a multibit ECC error occurred. | Error | Put the system into maintenance mode |

| Event Name | Description | Severity | Recommended Action |
|---|---|---|---|
| Dell - Fan enclosure inserted into system | Sensor returned to normal value. | Info | No action |
| Dell - Fan enclosure removed from system | A fan enclosure has been removed from the specified system. | Warning | No action |
| Dell - Fan enclosure removed from system for an extended amount of time | A fan enclosure has been removed from the specified system for a user-definable length of time. | Error | No action |
| Dell - Fan enclosure sensor detected a non-recoverable value | A fan enclosure sensor in the specified system detected an error from which it cannot recover. | Error | No action |
| Dell - AC power has been restored | Sensor Returned to Normal Value. | Info | No action |
| Dell - AC power has been lost warning | An AC power cord has lost its power, but there is sufficient redundancy to classify this as a warning. | Warning | No action |
| Dell - An AC power cord has lost its power | An AC power cord has lost its power, and lack of redundancy requires this to be classified as an error. | Error | No action |
| Dell - Processor sensor returned to a normal value | Sensor Returned to Normal Value | Info | No action |
| Dell - Processor sensor detected a warning value | A processor sensor in the specified system is in a throttled state. | Warning | No action |

| Event Name | Description | Severity | Recommended Action |
|---|---|---|---|
| Dell - Processor sensor detected a failure value | A processor sensor in the specified system is disabled, has a configuration error, or experienced a thermal trip. | Error | No action |
| Dell - Processor sensor detected a non-recoverable value | A processor sensor in the specified system has failed. | Error | No action |
| Dell - Device configuration error | A configuration error was detected for a pluggable device in the specified system. | Error | No action |
| Dell - Battery sensor returned to a normal value | Sensor Returned to Normal Value | Info | No action |
| Dell - Battery sensor detected a warning value | A battery sensor in the specified system detected that a battery is in a predictive failure state. | Warning | No action |
| Dell - Battery sensor detected a failure value | A battery sensor in the specified system detected that a battery has failed. | Error | No action |
| Dell - Battery sensor detected a non-recoverable value | A battery sensor in the specified system detected that a battery has failed. | Error | No action |

| Event Name | Description | Severity | Recommended Action |
|---|---|---|---|
| Dell - Thermal shutdown protection has been initiated | This message is generated when a system is configured for thermal shutdown due to an error event. If a temperature sensor reading exceeds the error threshold for which the system is configured, the operating system shuts down and the system powers off. This event may also be initiated on certain systems when a fan enclosure is removed from the system for an extended period of time. | Error | No action |
| Dell - Temperature sensor returned to a normal value | Sensor Returned to Normal Value. | Info | No action |
| Dell - Temperature sensor detected a warning value | A temperature sensor on the backplane board, system board, CPU, or drive carrier in the specified system exceeded its warning threshold. | Warning | No action |
| Dell - Temperature sensor detected a failure value | A temperature sensor on the backplane board, system board, or drive carrier in the specified system exceeded its failure threshold value. | Error | Put the system into maintenance mode |

| Event Name | Description | Severity | Recommended Action |
|---|---|---|---|
| Dell - Temperature sensor detected a non-recoverable value | A temperature sensor on the backplane board, system board, or drive carrier in the specified system detected an error from which it cannot recover. | Error | No action |
| Dell - Fan sensor returned to a normal value | Sensor Returned to Normal Value | Info | No action |
| Dell - Fan sensor detected a warning value | Fan Sensor reading in the host <x> exceeded a warning threshold value. | Warning | No action |
| Dell - Fan sensor detected a failure value | A fan sensor in the specified system detected the failure of one or more fans. | Error | Put the system into maintenance mode |
| Dell - Fan sensor detected a non-recoverable value | A fan sensor detected an error from which it cannot recover. | Error | No action |
| Dell - Voltage sensor returned to a normal value | Sensor Returned to Normal Value | Info | No action |
| Dell - Voltage sensor detected a warning value | A voltage sensor in the specified system exceeded its warning threshold | Warning | No action |
| Dell - Voltage sensor detected a failure value | A voltage sensor in the specified system exceeded its failure threshold. | Error | Put the system into maintenance mode |

| Event Name | Description | Severity | Recommended Action |
|---|---|---|---|
| Dell - Voltage sensor detected a non-recoverable value | A voltage sensor in the specified system detected an error from which it cannot recover. | Error | No action |
| Dell - Current sensor returned to a normal value | Sensor Returned to Normal Value. | Info | No action |
| Dell - Storage: storage management error | Storage management has detected a device independent error condition. | Error | Put the system into maintenance mode |
| Dell - Storage: Controller warning | A portion of the physical disk is damaged. | Warning | No action |
| Dell - Storage: Controller failure | A portion of the physical disk is damaged | Error | Put the system into maintenance mode |
| Dell - Storage: Channel Failure | Channel failure. | Error | Put the system into maintenance mode |
| Dell - Storage: Enclosure hardware information | Enclosure hardware information. | Info | No action |
| Dell - Storage: Enclosure hardware warning | Enclosure hardware warning. | Warning | No action |
| Dell - Storage: Enclosure hardware failure | Enclosure hardware error. | Error | Put the system into maintenance mode |
| Dell - Storage: Array disk failure | Array disk failure. | Error | Put the system into maintenance mode |
| Dell - Storage: EMM failure | EMM failure. | Error | Put the system into maintenance mode |
| Dell - Storage: power supply failure | Power supply failure. | Error | Put the system into maintenance mode |

| Event Name | Description | Severity | Recommended Action |
|---|---|---|---|
| Dell - Storage: temperature probe warning | Physical disk temperature probe warning, too cold or too hot | Warning | No action |
| Dell - Storage: temperature probe failure | Physical disk temperature probe error, too cold or too hot. | Error | Put the system into maintenance mode |
| Dell - Storage: Fan failure | Fan failure. | Error | Put the system into maintenance mode |
| Dell - Storage: Fan failure | Fan failure. | Error | Put the system into maintenance mode |
| Dell - Storage: Battery warning | Battery warning. | Warning | No action |
| Dell - Storage: Virtual disk degraded warning | Virtual disk degraded warning. | Warning | No action |
| Dell - Storage: Virtual disk degraded failure | Virtual disk degraded failure. | Error | Put the system into maintenance mode |
| Dell - Storage: Temperature probe information | Temperature probe information | Info | No action |
| Dell - Storage: Array disk warning | Array disk warning. | Warning | No action |
| Dell - Storage: Array disk information | Array disk information. | Info | No action |
| Dell - Storage: Power supply warning | Power supply warning. | Warning | No action |

# Index


## C

connection profiles
  create new, 48

contacting Dell, 100

create new
  connection profiles, 48
  hardware profiles, 65
  hypervisor profiles, 70

## D

Dell
  contacting, 100

Dell plug-in
  database backup and restore, 89
  uninstalling, 39
  upgrade, 40
  What is it?, 9

deployment templates
  managing, 72

deployment wizard
  overview, 73

documentation
  Dell PowerEdge servers, 100
  Lifecycle Controller (LCC), 101
  OpenManage Server
    Administrator (OMSA), 100
  VMware vSphere, 100

## F

features
  high-level functionality, 9

firmware
  scheduling updates, 79
  updates for Dell hardware, 9

## G

glossary
  Dell corporate, 100

## H

hardware faults
  alerting, 9

hardware management, 45

hardware profiles
  create new, 65
  managing, 68

hypervisor profiles
  create new, 70
  managing, 71

## I

inventory
  displays in vCenter, 9

## L

LCC - Lifecyle Controller
documentation, 101

## M

managing
deployment templates, 72
hardware profiles, 68
hypervisor profiles, 71

## O

OMSA - OpenManage Server Administrator
documentation, 100

overviews
deployment wizard, 73
zero-touch provisioning/deployment, 62

## P

phone numbers, 100

plug-in, *see* Dell plug-in

PowerEdge servers
documentation, 100

## R

remote operations
deployment and provisioning, 10

## S

scheduling
server firmware updates, 79

server deployment
states, 63
using profiles, 10

servers
deployment states, 63
scheduling firmware updates, 79

support
contacting Dell, 100

system event logs
displaying, 54

## T

telephone numbers, 100

terminology
Dell corporate, 100

## U

uninstalling
Dell plug-in, 39

upgrade
Dell plug-in, 40

## V

VMware
vSphere documentation, 100

## W

warranty information
  Dell online, 10